FORSVARET
Forsvarets høgskole

Småstaten Norge – en cyberstormakt?

En komparativ analyse av israelsk og norsk cybermakt

Ken-Richard Brunstad

Masteroppgave

Forsvarets høgskole

Vår 2018

- BLANK SIDE -

Forord

Først og fremst vil jeg takke mine veiledere, Kristin Hemmer Mørkestøl og Rolf Tamnes, for inspirasjon, gode råd, og for å ha utvist tålmodighet og utholdenhet når jeg både bommet på skiva og levert forsinkede kapittelutkast. Videre fortjener bibliotekets ansatte ros for sin serviceinnstilling.

Aller mest vil jeg takke Tonje, min kone. Takk for at du nok en gang har tatt deg av alt når jeg har vært opptatt med mitt. Til sist en unnskyldning til mine to sønner som har fått mye mindre oppmerksomhet enn fortjent. Det skal bli bedre nå.

Sammendrag

Denne oppgaven er en kvalitativ og komparativ analyse av norsk og israelsk cybermakt og handler om hvilke konsekvenser utviklingen av cybermakt har for Norges evne til forsvar, suverenitetshevdelse og myndighetsutøvelse. Oppgavens tittel indikerer hovedproblemet: Kan Norge endre nåsituasjonen - som i en rekke offentlige utredninger og uttalelser beskrives som avmakt - til å bli en cyberstormakt? For høydigitaliserte samfunn med nettverksbasert forsvarsevne oppleves digitaliseringens muligheter også som en akilleshæl. Israel, en småstat med noen grunnleggende likheter med Norge, har snudd avmakt til makt. Den komparative analysen har sett på forskjeller og likheter mellom israelsk og norsk organisering av cybermakt og prinsipper for anvendelse av cybermakt. Studien har funnet at det er tre sentrale forskjeller mellom israelsk og norsk organisering. 1) Israel har etablert et sentralstyrt cyberdirektorat som styrer store deler av cyberpolitikken på en enhetlig måte – til forskjell fra Norge som har fordelt det samme ansvaret på flere departementer og en rekke direktorater. 2) Israel har etablert et militærindustrielt cyberkompleks som bidrar til å styrke statssikkerheten, samtidig som det fronter israelsk økonomisk vekst. Slikt er ukjent i Norge. 3) Israel har fordelt offensiv cybermakt på flere organisasjoner med ansvar for både stats- og samfunnssikkerhet. I tillegg anvender Israel offensiv cybermakt aktivt «mellom kriger» for å unngå krig og bidra til avskrekking, og landets anvendelse av cybermakt tjener statens grunnleggende målsetting: overlevelse. I Norge er både grunnleggende målsettinger og cybermaktens formål mer utydelig. Studien tar for seg tre scenarioer hvor norsk forsvar, suverenitet og myndighetsutøvelse utfordres av Russland og asymmetriske trusselaktører, og beskriver hvilke utfordringer det norske krisehåndteringssystemet, Forsvaret og politiet vil ha med å håndtere disse, med dagens kapasitet og organisering. Studien har vist at det *ikke* er realistisk at Norge kan bli en cyberstormakt som Israel, fordi offensiv opptreden i fredstid ikke er forenelig med norsk politikk og strategisk styrkeøkonomisering med basis i Forsvaret ikke er realistisk oppnåelig. Norge *kan* derimot snu avmakt til cybermakt. Dette kan først og fremst skje ved at norsk politikk på cyberområdet forenes med sikkerhetspolitiske målsettinger. Dernest ved at det investeres i sivil og militær cyberforsvarsevne som sikrer opprettholdelse av fellesoperativ kampkraft, utholdenhet og alliert mottak. Og sist men ikke minst ved satsing på alliert cybermakt som kan kontre motstanderes evne til å forstyrre handlefrihet og redusere utholdenhet allerede i tidlig konfliktfase.

Summary

This assignment is a qualitative and comparative analysis of Norwegian and Israeli cyber power and about the consequences the development of cyber power has for Norway's ability to defend, maintain sovereignty and exercise authority. The title of the thesis indicates the main problem: Can Norway change the current situation - described as powerlessness - to become a great cyber power? For highly digitized societies with network centric warfare capabilities, the digitization has also become an Achilles heel. Israel, a small state with some basic similarities with Norway, has revolved powerlessness to power. This comparative analysis has looked at differences and similarities between Israeli and Norwegian organization and principles for the use of cyber power. The study has found that there are three key differences between Israeli and Norwegian organizations. 1) Israel has established a centralized cyber-directorate that manages large parts of cyber policy in a unified manner - unlike Norway, which has shared the same responsibility in several ministries and a number of directorates. 2) Israel has established a military-industrial cyber complex that helps to strengthen state security while fostering Israel’s economic growth. Such is unknown in Norway. 3) Israel has distributed offensive cyber power to several organizations. In addition, Israel actively uses cyber power between wars to prevent war and contribute to deterrence. In addition, Israel’s use of cyber power serves the state's fundamental objective: survival. In Norway, both the basic objectives and the purpose of cyber power are more unclear. The thesis addresses three scenarios where Norwegian defence, sovereignty and authority are challenged by Russia and asymmetric threat actors, and describes the challenges the Norwegian crisis management system, the Armed Forces and the police will deal with – with today's capacity and organization. The study has shown that it is *not* realistic that Norway can become a great cyber power like Israel because offensive engagements in peace time is not companionable with Norwegian politics and strategic economy of force based on the Armed Forces is not realistically achievable. On the other hand, Norway *can* advance to cyber power. This can primarily be achieved by uniting Norwegian policy in the cyber area with security policy objectives. Secondly, by investment in civilian and military cyber defence capabilities that ensure the upkeep of joint operational battle force, endurance and allied reception. And last but not least, by aiming on allied cyber power that can counter opponents' ability to interfere with freedom of action and reduce endurance already at early conflict phases.

Innholdsfortegnelse

1 Innledning

Denne oppgaven omhandler cybermakt i småstatsperspektivet. Makt i internasjonale relasjoner har tradisjonelt vært relatert til statens militære kapabilitet, i en verden hvor småstater er kvantitativt underlegne stormakter. Småstater har derfor søkt å finne alternative maktmidler for å utjevne maktbalansen: teknologisk overlegenhet og utjevning av ubalanse gjennom allianser er blant disse. Flere har hevdet at småstater kan anvende cybermakt for å utjevne skjevheten i maktforholdet til stormakter (se for eksempel Rivera, 2015, s. 8-20), men det er muligens flere som har fremholdt det motsatte: at cybermakt ikke endrer maktforholdet mellom småstater og stormakter (se for eksempel Eggen, 2013, s. 2).
For en småstat som Norge er en sammenligning med Israel spesielt relevant av følgende grunner: Israel er også en småstat, men samtidig en cyberstormakt. Norge og Israel er begge høyteknologiske og digitaliserte land. Og til sist: Det kan finnes løsninger på norske utfordringer ved å studere israelsk cybermakt. En komparativ analyse av norsk og israelsk cybermakt har ikke blitt gjennomført tidligere, noe som også bidrar til studiens relevans.

1.1 Bakgrunn

Etterretningstjenesten og Politiets sikkerhetstjenestes (PST) trusselvurderinger for 2018 vektlegger fremmedstatlig etterretning som den største trusselen mot Norge og norske interesser (Etterretningstjenesten, 2018, s. 26-33; Politiets sikkerhetstjeneste, 2018, s. 7-13). Etterretningstjenesten fremhever i tillegg forberedelser til digital sabotasje og undergraving av norske interesser blant de største truslene. Norge utsettes daglig for digital spionasje og cyberangrep fra både russiske og kinesiske aktører. Digitaliseringen av Forsvaret og samfunnet, fremveksten av cyberdomenet som en arena for militære operasjoner, og avhengigheten av digitale verdikjeder har muliggjort etterretning, sabotasje og påvirkningsoperasjoner i en skala som mangler historisk motstykke. Verdensbildet er riktignok i endring, i vår del av verden med økt spenning mellom NATO og Russland, men fremmede staters økte mulighet til å bedrive etterretning, påvirkning og sabotasje skyldes i hovedsak at digitaliseringen har kostnadseffektivisert innhentingsmulighetene og redusert

muligheten for å bli oppdaget. Digitale operasjoner rettes mot norsk forsvars- og beredskapssektor, statsforvaltning, forskning og utvikling, og kritiske samfunnsfunksjoner. Fremmedstatlig cybermakt brukes i fredstid til spionasje, forberedelser til sabotasje og angrep og til undergravende virksomhet. Flere stater, deriblant USA, Russland, Kina og Israel har vist evne og vilje til å bruke cybermakt som et virkemiddel i militære operasjoner og væpnede konflikter for å oppnå egne politiske og militære målsettinger. Hva gjør Norge for å håndtere disse truslene?

I Norge har en rekke offentlige utredninger, *Samhandling for sikkerhet*, *Digital sårbarhet – sikkert samfunn* og *Digitalt grenseforsvar*, påpekt at hverken Cyberforsvaret, E-tjenesten, politiet eller Nasjonal sikkerhetsmyndighet, som alle har roller for ivaretakelse av stats- og samfunnssikkerheten mot cybertrusler, er bemidlet eller bemyndiget til å håndtere fremmedstatlig digital etterretning, sabotasje og subversjon (se Lysne, Grytting, Jarbekk, Lunde, & Reusch, 2016; NOU 2015:13; NOU 2016:19).

Småstaten Israel har på den annen side vist at den har evne til å utvikle og utøve cybermakt (inkludert forsvar, suverenitetshevdelse og myndighetsutøvelse), basert på tre prinsipper: strategisk styrkeøkonomisering; offensiv opptreden; og enhetlige strategiske målsettinger, samtidig som de styrker sin egen økonomiske situasjon.

Sammenlignet med Israel er Norge i dag en småstat innen cybermakt. Som jeg vil vise i analysen er Norges evne til å forsvare staten og samfunnet mot digitale trusler preget av følgende forhold: fag- og sektordeling, lav deteksjonsevne, svak evne til kriminalitetsbekjempelse, frivillighetsbasert beskyttelse av sivil infrastruktur, utdaterte lovverk og begrensede politiske målsettinger. Norsk *avmakt* i cyberdomenet står i sterk kontrast til israelsk *cybermakt*.

Norge er et av verdens mest digitaliserte land, og har i likhet med de fleste vestlige land valgt å føre en politikk hvor militærmakten tilpasser seg den digitale utviklingen i samfunnet og verden forøvrig. Norge har utviklet et nettverksbasert forsvar (NbF), med fokus på informasjonsoverlegenhet, etterretning og overvåkning, høyteknologiske langtrekkende presisjonsvåpen og femtegenerasjons kampfly. Norge har tilsynelatende satset på kvalitet –

teknologisk overlegenhet – fremfor kvantitet. Det er ikke nødvendigvis et motsetningsforhold mellom kvantitet og kvalitet – kvantitet skal sikres gjennom troverdig alliert støtte. Et lite, men høyteknologiske nettverksbasert forsvar må imidlertid kunne gi et komparativt fortrinn og utholdenhet nok til å holde tilbake et væpnet angrep – inntil USA og NATO kommer til unnsetning.

Mens USA og Storbritannia over tid har vært tydelige aktører på den globale cyberarenaen, er land som Kina og Russland nå i sterk utvikling på feltet. Russland, som fortsatt ser seg selv som teknologisk underlegen, har fokusert på utvikling av kapasiteter og evner som kan slå ut vestlig teknologi, i tillegg til en omfattende høyteknologisk oppbygging av øvrige stridskrefter (Ravndal, 2016, s. 30-39). De russiske kapasitetene omfatter både langtrekkende presisjonsvåpen (Askvik, 2015, s. 40-46), elektromagnetiske våpen, elektronisk krigføring (EK) og digital krigføring (Giles et al., 2015, s. 19-88). Russlands digitale krigføringskapasitet består av påvirkningsoperasjoner, spionasje og sabotasje (Etterretningstjenesten, 2018, s. 30). Til nyere tids russisk doktrine hører nå elementer som «electronic knockdown» (Chekinov & Bogdanov, 2013, s. 13-21) og «information activities» (Gerasimov, 2016, s. 23 - 28) som gjennomgående maktmidler i russisk maktutøvelse i fred, krise og krig[1]. Russland har demonstrert sin evne til å holde et høyt tempo og integrere ukonvensjonelle maktmidler i operasjonene i både Ukraina og Syria (Etterretningstjenesten, 2017b, s. 11-37). Russisk evne til hybrid krigføring, det vil si å synkronisere ukonvensjonelle maktmidler med den militære kampanjen, argumenteres av mange å være den nye russiske doktrinen – gjerne referert til som Gerasimovdoktrinen. Men ser man Russlands tre største militære kampanjer de siste ti årene under ett så har Russland fulgt ulike operasjonsmønstre i Georgia, Ukraina og Syria. Man kan med andre ord ikke utelukke at Russland vil gjøre noe annet i neste konflikt. Samtidig vil det være ulogisk å anta at Russland ikke vil bruke sin velutviklede evne innen EK og cybermakt for å utjevne skjevheten i en eventuell konflikt mellom Russland og NATO. Den norske forsvarsevnen kan derfor forventes å bli sterkt utfordret av russisk EK og cybermakt.

[1] Både Chekinov & Bogdanov og Gerasimovs artikler er basert på observasjoner av vestlig krigføring i perioden 1990 til 2013. Chekinov og Bogdanov beskriver «electronic knockdown» som en innledende offensiv med kombinert bruk av EK og digitale operasjoner for å forme stridsmiljøet. Gerasimovs «Information activities» brukes gjennomgående i alle faser om både militære og ikke-militære aktiviteter for å påvirke informasjonsmiljøet, og inkluderer ulike former for påvirkning, etterretning og sabotasje.

Ved siden av stormaktene USA, Storbritannia, Russland og Kina skiller Israel seg ut som det landet som har kommet lengst i utviklingen av cybermakt. Krigerstaten, omringet av fiender og i stadig konflikt med araberstatene, har blitt et land som det vises til når cybermakt skal utvikles (Netanyahu, 2016).

1.2 Problemstillinger

Cyberdomenet er nå anerkjent som et militært operasjonsdomene på linje med land-, luft- og sjødomenene (NATO, 2016c, 2016b). Fremtidige konflikter forventes å bli sterkt preget av at motstandere utfordrer hverandre også i og gjennom det digitale rom. Norge er et av verdens mest digitaliserte land, Forsvaret er blitt heldigitalisert og innrettet etter NbF-tenkningen, og digitaliseringens bakside, sårbarheter og digitale trusler, får stor oppmerksomhet i Norge. Men digitaliseringen og de medfølgende sårbarhetene er ikke unikt for Norge. Israel har evnet å snu situasjonen og gjort sårbarhetene som følger med digitaliseringen om til en styrke. Israel har gått fra fokus på IKT-sikkerhet til cybermakt (Tabansky, 2016a, s. 110-113, 2016b, s. 51-63). Har Norge forutsetninger for å gjøre som Israel: kan Norge snu avmakt til cybermakt? For å svare på dette vil følgende tre problemstillinger utforskes:

1. Hva kjennetegner israelsk og norsk cybermakt?
2. Hvilke likheter og forskjeller finnes mellom israelsk og norsk cybermakt?
3. Hvilke erfaringer kan hentes fra Israels utøvelse av cybermakt for utviklingen av norsk cybermakt?

For å forklare forskjeller mellom norsk og israelsk cybermakt skal vi først studere hvilke faktorer Israels cybermakt bygger på, for deretter å analysere betydning av cybermakt innen tre kjerneoppgaver for Norges sikkerhet:

- Forsvar mot angrep
- Suverenitetshevdelse
- Myndighetsutøvelse

Disse tre kjerneoppgavene utgjør de sammenlignbare variablene i den komparative analysen. Variablene er generelle og vil kunne brukes på de fleste nasjonalstater, men inneholder også forskjellige tolkninger og meninger fra stat til stat. Cybermakt er et komplekst og for de fleste uoversiktlig felt. Jeg har derfor sett behov for å *beskrive* virksomheten utførlig i hele sin bredde, som et nødvendig grunnlag for drøftingen.

1.3 Avgrensning

Temaet cybermakt er i de fleste land omsluttet av hemmelighold. Det har siden starten vært et mål at denne studien skulle være tilgjengelig for flere enn forfatteren selv og veilederne, og denne baserer seg derfor kun på åpne kilder. Dette er også en av de største svakhetene med studien: Enkelte relevante poenger på norsk side har måttet utelates av hensyn til sikkerhetsgradering. Enkelte viktige poenger på israelsk side er helt sikkert utelatt med bakgrunn i forfatterens manglende innsyn.

Med bakgrunn i at det finnes mer litteratur om sivile elementer innen cybermakt enn de militære avdelingenes utøvelse av cybermakt, har sivil organisering og kapasitet blitt fremstilt mer detaljert enn de militære organisasjoner og kapasiteter. En svakhet med kildematerialet er at israelsk litteratur ofte er positivt vinklet, mens den norske litteraturen ofte er negativt vinklet, noe som potensielt kan påvirket analysen.
En annen svakhet med studien er at forfatteren selv ikke behersker hebraisk og dermed kan ha gått glipp av relevant forskning som kunne kastet ytterligere lys over problemstillingen.

Studien avgrenser seg til tre av Forsvarets oppgaver: forsvar, suverenitetshevdelse og myndighetsutøvelse. Forsvarets øvrige oppgaver blir ikke grundig belyst.

1.4 Teori og sentrale begreper

I det videre beskrives småstatsteorien som er lagt til grunn for analysen, og de viktigste begrepene knyttet til cybermakt blir beskrevet og diskutert.

1.4.1 Småstater og stormakter

I den klassiske realismen etter 2. verdenskrig er stater gjerne blitt klassifisert etter militær kapabilitet. Norge er uten tvil en småstat i den klassiske realismen. For Israel betoner det seg annerledes, selv om det også vil havne et stykke ned på en slik kvantitativ måling. For eksempel vurderes Israel som verdens 16. mektigste militærmakt basert på en kvantitativ kalkyle (GFP, 2018).

Men det finnes også kvalitative måter å måle staters makt på. Dersom man vurderer faktorer som politisk innflytelse, diplomatisk påvirkningskraft og økonomi, blir regnestykket annerledes. En stat kan utøve påvirkning og innflytelse på avgrensede områder, og en småstat kan regnes som en stormakt innen segmenter. Norge var i 2003 nummer ni på Newsweeks rangering av verdens mektigste land, med begrunnelsen «A high quality of life and diplomatic prestige.» (Løvold, 2004, s. 9). Newsweeks rangeringer er basert på en kvalitativ vurdering av en rekke faktorer, som utdanning, økonomi, militær styrke, folketall, innovasjon etc.

Ifølge Aron (1966, s. 83) forsøker småstater mest av alt å overleve i det internasjonale systemet. Det vil være ulogisk av en militær småstat å utfordre en militær stormakt offensivt med militære midler. Men dersom vi også trekker inn andre maktfaktorer, som diplomati, økonomi, informasjons- og cybermakt, kan småstater tillate seg å utøve makt, innflytelse eller påvirkning innenfor avgrensede områder. Ergo kan også småstater være store innen enkelte maktsegmenter og også ha offensiv makt.

Dersom vi aksepterer argumentet at cybermakt kan påvirke de klassiske maktfaktorene som diplomati, informasjonsmakt, militær- og økonomisk makt (se punkt 1.4.3), vil en småstat som er en cyberstormakt (teoretisk sett) kunne utfordre og redusere andre staters makt også på

andre arenaer enn cybermakt. Israels cyberangrep på Irans atomvåpenprogram er et eksempel på bruk av cybermakt for å redusere en annen stats militære makt.[2] Israels storstilte cyber-innovasjon og eksport av cybersikkerhet er et eksempel på hvordan det øker egen økonomisk makt ved hjelp av cybermakt.

Et annet relevant perspektiv som cybermakt bringer til diskusjonen om småstater og stormakter, er at alle verdens stater kan regnes som nabostater i cyberdomenet, og at geopolitisk avstand dermed har mindre betydning enn tidligere. Det betyr at ingen stater kan vurderes som en *regional* cyberstormakt (eller -småstat), og at cybermakten er global. Dette skiller seg vesentlig fra klassisk militær makt i landdomenet spesielt.

Om vi benytter den klassiske realismens kvantitative hierarkiske maktrangeringsprinsipp, forblir Israel en småstat (eller mellomstor stat). At Israel likevel anses som en stor cybermakt, har ikke bare utspring i deres demonstrerte offensive evne (operasjon Olympic Games og operasjon Orchard[3]), men like mye i satsningen på cybersikkerhet, innovasjon, industri og strategi (Tabansky, 2016b, s. 57-59). Det ligger med andre ord en kvalitativ logikk til grunn for argumentet om at småstater kan være stormakter innen enkeltsegmenter - i dette tilfellet cybermakt.

Det finnes ingen generell småstatsteori som forklarer hvordan småstater oppfører seg når vi tar utgangspunkt i det kvalitative maktbegrepet. «Betydningen av kategorien *småstat* bestemmes av den politiske orden den er en del av.» (Løvold, 2004, s. 24-25). For småstaten og «fredsnasjonen» Norge, som innen småastatsrealismen utøver makt og innflytelse gjennom internasjonal orden, demokrati og fred, vil ikke nødvendigvis cybermakt ha samme betydning

[2] Operasjon Olympic Games ble angivelig gjennomført av USA og Israel for å hindre Iran å utvikle atomvåpen. Operasjonen skal ha vært planlagt og forberedt over flere år, før skadevaren Stuxnet ble oppdaget. Stuxnet lyktes å trenge inn i Irans lukkede atomvåpen program og påføre mekanisk ødeleggelse av anrikingssentrifugene i 2010. Cyberangrepet skal ha satt Irans atom-program flere år tilbake i tid. Stuxnet var et presisjonsvåpen, og medførte ingen annen skade selv om skadevaren spredde seg globalt (se Anderson & Sadjadpour, 2018, s. 9).

[3] Operasjon Orchard er et av de første kjente tilfellene hvor cybermakt ble synkronisert med konvensjonelle militære maktmidler. I september 2007 bombet israelske F-15 og F-16 et atomanlegg nord i Syria. Operasjonen skal ha blitt muliggjort av et cyberangrep som satte det syriske luftvernsystemet ut av spill (se Rid, 2012, s. 16).

som for «krigerstaten» Israel. For Israel har den overordnede strategiske målsettingen vært å sikre statens eksistens. Israel har derfor møtt enhver krig og konflikt som en eksistensiell trussel. Offensiv opptreden, på alle arenaer – også i cyberdomenet – for å akkumulere avskrekking, er en etablert del av det israelske forsvarets (Israeli defence forces, heretter IDF) strategi. Det hører til både etablert militær teori og Israels strategi at defensivt forsvar alene ikke kan bekjempe trusler (Israeli Defence Forces, 2016, s. 10). Når vi da i det videre skal sammenligne og analysere Norge og Israels cybermakt, må det gjøres i konteksten av de svært ulike politiske landskapene de er en del av.

1.4.2 Cyberdomenet

Om vi skal forstå cybermakt, må vi også forstå cyberdomenet. En omforent definisjon av cyberdomenet finnes fortsatt ikke (NATO Cooperative Cyber Defence Centre of Excellence, 2018). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren* (heretter *FDs cyberretningslinjer*) definerer cyberdomenet som: «Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data.» (Forsvarsdepartementet, 2014, s. 5). Debatten om hva cyberdomenet er og hva begrepet inneholder, drives av både politiske, militære og kommersielle krefter (se for eksempel Langø, 2013). Cyberdomenet sidestilles gjerne med det digitale rom, og omtales i mange sammenhenger som et digitalt domene, med en eller annen knytning til informasjon, teknologi og mennesker (Etterretningstjenesten, 2018, s. 30; Inglis, 2016, s. 19-26; Johnsen, 2014, s. 7; Rid, 2012, s. 164-165).

Om det elektromagnetiske spektrum[4] er en del av eller knytter sammen cyberdomenet, er en pågående diskusjon. Den pågående utviklingen som fusjonerer IT og radioteknologi taler for at en bås-tankegang om digitale og elektromagnetiske virkemidler kan være både vitenskapelig og militært ufordelaktig. Cyber er et begrep som i dag forstås forskjellig over alt, eller som Thomas Rid (2015) sier det: «in Tel Aviv, it triggers visions of humans merging with machines, of wired-up prostheses with sensitive fingertips, and of silicon chips implanted under tender human skin.»

[4] Det elektromagnetiske spektrum er definert som en egen *dimensjon* og et *operasjonsmiljø* i FFOD (Forsvarsstaben, 2014, s. 23).

Når *cyberdomenet* omtales i denne studien, inneholder begrepet både *det digitale rom* og *det elektromagnetiske spektrum*.

1.4.3 Cybermakt

Hva er cybermakt? Hva kan cybermakt anvendes til? Dette avsnittet søker å gi en definisjon på cybermakt.

For å finne kjernen i den komparative studien har det vært nødvendig å definere det flyktige og uetablerte begrepet cybermakt. Denne studien tar utgangspunkt i cybermakt som et maktmiddel for stater på den internasjonale arenaen. I tradisjonell forstand er det forsvaret som skal ivareta statens sikkerhet mot ytre trusler, mens politiet har ansvar for samfunnssikkerheten og indre sikkerhet. I Norge har vi tilstrebet et skarpt skille mellom politi og forsvar. Cyberdomenet bidrar til å viske ut dette skillet, og cybermakt må da forstås i en helhetlig sammenheng.

Staters makt er tradisjonelt blitt målt i hvilken evne en stat har til å tvinge gjennom sin vilje overfor andre stater, med militærmakten som det ultimate maktmiddel. Blant stormaktene eksisterer denne oppfatningen i stor grad den dag i dag. Gelb (2009, s. 28) definerer makt som «getting people or groups to do something they don't want to do».

For cybermakt kan dette omsettes til: «the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power[5]» (Kuehl, 2009, s. 184). En definisjon som også brukes i Israel (Tabansky & Ben-Israel, 2015, s. 3).

[5] En vanlig måte å klassifisere maktinstrumenter på er diplomatisk-, informasjons-, militær- og økonomisk makt (DIME).

1.4.4 Cyberoperasjoner, digitale operasjoner og elektronisk krigføring

FDs cyberretningslinjer beskriver cyberoperasjoner/datanettverksoperasjoner/computer network operations (CNO) som:

> «tiltak som gjennomføres i datanettverkene for å påvirke motstanders datanett og beskytte eget nett. Dette omfatter Computer Network Defence (CND), Computer Network Exploitation (CNE) og Computer Network Attack (CNA) … Cyberoperasjoner omfatter ikke tiltak utenfor datanettverkene for å påvirke disse, eksempelvis i form av kinetiske maktmidler og elektronisk krigføring.» (Forsvarsdepartementet, 2014, s. 5-6).

Etter FDs definisjon skiller vi elektronisk krigføring, og dermed også det elektromagnetiske spektrum, fra cyberdomenet. Med den alternative måten å definere cyberdomenet på som bestående av *det digitale rom* og *det elektromagnetiske spektrum* vil digitale operasjoner og elektronisk krigføring (EK) være to forskjellige disipliner innen cybermakt - slik som infanteri og artilleri er innen landmakt.[6] Både den pågående teknologiutviklingen og konsepter som «multi-domain battle» er argumenter for at en slik tilnærming kan være hensiktsmessig (Ben-israel & Tabansky, 2011, s. 27-29; van Niekerk & Maharaj, 2009, s. 10-11). For eksempel melder enkelte kilder at amerikanske F-35 vil ha offensive kapasiteter som kombinerer digitale operasjoner med EK (Clark, 2016). Dette sammen med utviklingstrekk innen kunstig intelligens, robotisering og kvantemekanikk antyder at vi fortsatt er på et tidlig stadium i vår forståelse av cyberdomenet, og at fremtiden kan by på flere krigføringsdisipliner innen cybermakt. Når cyberoperasjoner omtales i denne studien handler det om både digitale og elektromagnetiske operasjoner.

1.4.5 Suverenitet og myndighetsutøvelse

Under beskrives de tre begrepene suverenitet og myndighetsutøvelse som benyttes i analysen av israelsk og norsk cybermakt, og som også danner grunnlaget for scenariobeskrivelsen i kapittel 4.

---

[6] USA er et av landene som er i gang med fusjonering av digitale og elektromagnetiske operasjoner. Se for eksempel *FM 3-12 Cyberspace and electronic warfare operations* (US Army, 2017).

Hverken Norge eller Israel har klare definisjoner som tydeliggjør hva statens suverenitet, suverene rettigheter eller suverenitetshevdelse i cyberdomenet innebærer. FN har heller ikke kommet til unison enighet om hva suverenitet innebærer for cyberdomenet (FN, 2018a).[7] Norge mener at gjeldende internasjonal rett og FN-traktaten også gjelder for cyberdomenet (Regjeringen, 2017, s. 1). Israel har ikke eksplisitt uttrykt sitt standpunkt i FN.[8]

Evne til innsats - Strategisk konsept for Forsvaret definerer *suverenitetshevdelse* som å «forsvare, om nødvendig med militærmakt, norske grunnrettigheter som stat mot andre stater som direkte eller indirekte utfordrer norsk suverenitet på norsk territorium, eller norske suverene rettigheter i norske jurisdiksjonsområder utenfor norsk territorium.» (Forsvarsdepartementet, 2009, s. 23). I *FDs cyberretningslinjer* slås det fast: «Forsvarets primæroppgaver er å hevde Norges suverenitet og suverene rettigheter, og forsvare landet mot ytre angrep (statssikkerhet). Det er regjeringen som avgjør om et cyberangrep skal ansees å være et væpnet angrep.» (Forsvarsdepartementet, 2014, s. 11). Og videre at:

> «[cyberangrep kan] regnes som ulovlig maktbruk etter FN-paktens artikkel 2(4). …Et angrep i cyberdomenet kan utløse en stats rett til selvforsvar etter FN-paktens artikkel 51. Terskelen er høy, og vil eksempelvis først gjelde der staten er utsatt for et omfattende angrep rettet mot kritisk infrastruktur, eller dersom cyberangrepet forårsaker betydelig tap av liv eller materiell skade.» (ibid, s. 13-14).

Forsvarets strategiske konsept fremholder videre at *suverene rettigheter* innebærer «Norges avgrensede rettigheter, basert på internasjonal rett og internasjonale avtaler … Begrepet er særlig relevant i områder der Norge ikke har territoriell suverenitet.» (Forsvarsdepartementet, 2009, s. 23).For Israel stiller det seg annerledes. IDFs militære strategi fastholder at:

> «The basic idea in the use of offensive force in the Operation Between Wars[9] is a combination of:

[7] Informasjonssikkerhet, og senere cybersikkerhet, i rammen av internasjonal sikkerhet har siden 1995 vært på FNs agenda i nedrustningsarbeidet.

[8] Selv om Israel ikke har uttrykt seg eksplisitt deltok det i 2014-2015 som en av 20 FN-nasjoner i en ekspertgruppe som blant annet utredet «Norms, rules and principles for the responsible behaviour of States» (FN, 2015).

[9] Operations Between Wars brukes om militære rutinemessige operasjoner i fredstid.

a. Covert and Clandestine operations[10] in all arenas and dimensions outside the borders of Israel. This is based on intelligence, for the purpose of damaging the enemy's efforts and initiatives.

b. Overt operations to create deterrence – demonstrates the limits of Israel's restraint.

While promoting legitimacy for actions of Israel and upholding on-going efforts to defend Israel's sovereignty.» (Israeli Defence Forces, 2016, s. 28)

Israels tolkning av FN-paktens artikkel 2(4) og 51 skiller seg med andre ord vesentlig fra Norges, og åpner for retten til å bruke offensiv militærmakt, i alle domener, med både skjulte, nektbare og synlige midler også i fredstid for å hevde sin suverenitet.

Mens suverenitet handler om internasjonal rett, handler myndighetsutøvelse om nasjonal rett. For Norge om norsk lov. For Israel om israelsk lov. Myndighetsutøvelse er normalt et ansvar for politiet og sivile myndigheter både i Norge og Israel. Men ingen regel er uten unntak. For eksempel utøver Forsvaret i Norge begrenset myndighet ved hjelp av kystvakten og grensevakten på vegne av Justis- og beredskapsdepartementet (og andre departement).

I denne studien brukes følgende definisjon av myndighetsutøvelse, basert på Forsvarets strategiske konsept, i både norsk og israelsk kontekst:

> «håndhevelse av påbud, forbud og andre vilkår, i henhold til lover, forskrifter eller annet gyldig kompetansegrunnlag, rettet mot enkeltpersoner eller andre private rettssubjekter. … Maktanvendelse mot en ytre fiende støter «ikke an mot legalitetsprinsippet i norsk rett», men suverenitetsprinsippet i internasjonal rett.» *(Forsvarsdepartementet, 2009, s. 24).*

Ytre fiender inkluderer i denne sammenheng fremmedstatlige cybertrussel-aktører.

[10] I IDFs strategi definert som: «**Covert operations** – planned and carried out so as to hide the identity of the party behind them, or to grant denial possibilities. Results are visible to the enemy. **Clandestine operations** – carried out in a way to ensure total concealment. The enemy should not even suspect that such an operation has ever taken place.» (Israeli Defence Forces, 2016, s. 28)

1.5 Metode og kilder

Denne kvalitative oppgaven kombinerer casestudier (også kalt tilfellestudier) og komparative studier. Casestudier kan forstås som intensive undersøkelser av et lite antall tilfeller som kan være alt fra individer, organisasjoner, land eller hendelser og beslutninger (Ringdal, 2013, s. 170). I komparative studier kalles caser gjerne analyseenheter. Analyseenhetene er i denne sammenhengen de to landenes cybermakt som sammenlignes, nemlig norsk og israelsk cybermakt.

For å forklare forskjeller mellom norsk og israelsk cybermakt skal vi først studere hvilke faktorer Israels cybermakt bygger på, for deretter å analysere betydningen av cybermakt innen tre kjerneoppgaver for Norges sikkerhet:

- Forsvar mot angrep
- Suverenitetshevdelse
- Myndighetsutøvelse

Disse tre kjerneoppgavene utgjør altså de sammenlignbare variablene i den komparative analysen. Casestudier og komparativ design kan basere seg på både kvantitativ og kvalitativ dataanalyse, men når variablenes innhold rommer flere tolkninger (slik som de gjør i de fleste sammenligninger mellom stater) kan en kvantitativ analyse være uhensiktsmessig (Ringdal, 2013, s. 185). Studien baserer seg derfor en på kvalitativ analyse av variablene.

Komparative studier har tradisjonelt blitt gjennomført som dybdestudier av analyseenhetenes politikk, samfunn og historie. Denne type dybdestudier krever både språk-kunnskap og feltarbeid. Men i samfunnsvitenskapen har det også vokst frem en studieretning innenfor komparative studier hvor en søker å kunne bruke mer generelle analyser. I boken *Paradigms and sand castles* forklarer Barbara Geddes (2003, s. 175-185) hvordan komparative studier kan kombineres med teorien om «rational choice». Geddes argumenterer for at denne kombinasjonen er enklere, hurtigere og krever lavere kostnader enn tradisjonelle studier.

1.5.1 Litteratur

Problemstillingene berører både sikkerhetspolitikk, militær teori, strategi og doktrine, og ikke minst cybermakt. Pålitelig kildemateriale på et tidsaktuelt fagfelt, hvor mange også kan ha egeninteresse av å fremme egne agendaer, krever inngående kildekritikk. Når kildeomfanget er så stort er det i tillegg behov for en metode for systematisk og analytisk kildekritikk. Jeg har valgt å bruke politiets og etterretningstjenestens metodikk for bearbeiding av informasjon og kildekritikk som grunnlag for litteraturstudien.[11]

Følgende skala hentet fra *Etterretningsdoktrinen* er benyttet som grunnlag for vurderinger av pålitelighet og riktighet i artikler og kilder:

	Pålitelighet[12]		Riktighet[13]
A	Fullstendig pålitelig	1	Bekreftet av andre kilder
B	Vanligvis pålitelig	2	Sannsynligvis riktig
C	Noenlunde pålitelig	3	Muligens riktig
D	Ikke vanligvis pålitelig	4	Tvilsom
E	Upålitelig	5	Lite sannsynlig (usannsynlig)
F	Påliteligheten kan ikke bedømmes	6	Riktigheten kan ikke bedømmes

Tabell 1: Evaluering av kilders pålitelighet og riktighet, hentet fra *Etterretningsdoktrinen* (s. 24), av Etterretningstjenesten, 2013, Oslo

1.6 Forskningsstatus

[11] Doktrinen er basert på AJP-2.1 (NATO, 2016a). Se også politiets etterretningsdoktrine (Politidirektoratet, 2014) som er tilpasset Forsvaret og NATO.

[12] I vurderingen av *pålitelighet* er lagt til grunn faktorer som forfatterens kvalifikasjoner, om forfatteren er betraktet som anerkjent og kunnskapsrik, organisasjonstilknytning og om uavhengige eksperter har kvalitetsvurdert informasjonen (fagfellevurdering).

[13] I vurderingen av riktighet er det tatt hensyn til når kilden ble publisert (eller revidert), om informasjonen er utdatert, om informasjonen er faktabasert eller basert på meninger, om informasjonen er nøyaktig og detaljert eller omfattende, samt bruk av kildehenvisning, referanseliste og bibliografi.

Cybermakt er forsket mye på i de siste årene. Det meste omhandler teknologi, mindre handler om makt. Israel har vært en foregangsnasjon på området. Det er likevel begrenset med materiale som beskriver det militære instrumentet, mens det er gode kilder på sivil side. En sammenligning av norsk og israelsk cybermakt har ikke blitt gjennomført tidligere.

Studien har lagt hovedvekt på artikler og bøker fra general og forsker Isaac Ben-Israel, og Dr. Lior Tabansky. Deres bøker og artikler gir innsikt i den israelske utviklingen av cybermakt fra midten av 1990-tallet til 2015. I tillegg har jeg benyttet meg av en rekke åpne kilder og følgende relevante offentlige dokumenter:

- *Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011*
- *Government Resolution No. 2443 of February 15, 2015: Advancing National Regulation and Governmental Leadership in Cyber Security*
- *Government Resolution No. 2444 of February 15, 2015: Advancing the National Preparedness for Cyber Security*
- *The Israeli Defence Forces Strategy*

Detaljert informasjon om organiseringen av Israels cyberkapabiliteter på militær side, er ikke offentlig tilgjengelig informasjon, og det finnes mye motstridende informasjon i forskjellige kilder. Studien begrenser seg derfor til hovedtrekkene som er verifiserbare fra flere kilder.

Studien av Norges cybermakt har lagt hovedvekt på NOUer og strategidokumenter, herunder blant annet:

- *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren (2014)*
- *NOU 2015:13 Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*
- *NOU 2016:19 Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*
- *Meld. St. 38 (2016-2017) IKT-sikkerhet: Et felles ansvar*
- *Nasjonal strategi for informasjonssikkerhet (2012)*

I tillegg til overnevnte har også en rekke forskningsartikler vært gjenstand for studie, blant annet fra Forsvarets Forsknings Institutt (FFI) og Norsk Utenriks Politisk Institutt (NUPI).

2 Komparativ analyse del I – Organisering av roller og ansvar for cybermakt

Norge og Israel er to stater med vidt forskjellige forutsetninger og målsettinger. Begge har en begrenset befolknings- og ressursbase, men god økonomi. Israel er omringet av fiender – Norge er i et rolig hjørne av verden på NATOs nordflanke. Norge lever i fred og frykter ikke krig (Epinion Norge, 2018, s. 4; Kantar TNS, 2017, s. 22). Israel har en målsetting om fred, men fokuserer på overlevelse (Israeli Defence Forces, 2016, s. 9). Israel har utkjempet 11 kriger siden opprettelsen i 1948 (de fleste av dem var av eksistensiell natur)[14]. Norge har ikke vært i krig siden 1945, men har deltatt i operasjoner og væpnede konflikter i andre deler av verden. Israel bruker ikke begrepet *fredstid*, men begrepet *mellom kriger*[15] (Israeli Defence Forces, 2016, s. 41; Leshem, 1998, s. 3-4; Rosenberg, 2016, s. 25).

NATO-alliansen, med USA som den fremste sikkerhetsgarantisten, er en forutsetning for norsk sikkerhet. USA er også en viktig alliert for Israel. Avskrekking er sentralt i både norsk og israelsk sikkerhetspolitikk. Norsk avskrekking er basert på troverdig alliert støtte og besittelse av høyteknologiske våpen. Israelsk avskrekking er en kumulativ prosess; besittelse av våpen er ikke nok. Demonstrasjon av evne og vilje til å bruke militær makt akkumulerer avskrekking over tid (Israeli Defence Forces, 2016, s. 27). Både Israel og Norge søker å forebygge krig. Når krig ikke kan unngås, er «defend and win» det mest sentrale militære prinsippet i israelsk strategi (Israeli Defence Forces, 2016, s. 17-18), om nødvendig uten hjelp utenfra. I norsk strategi er «forsvar» basert på «alliert støtte» det mest sentrale prinsippet (Forsvarsdepartementet, 2016a, s. 15).

[14] Israelske kriger og konflikter: Den første arabisk-israelske krig (1948–1949), Suezkrisen (1956), Seksdagerskrigen (1967), Utmattelseskrigen (1969–1970), Jom kippur-krigen (1973), Første Libanon-krig (1982–1985), Første intifada (1987–1992), Andre intifada (2000–ca. 2005), Andre Libanon-krig (2006), Gaza-konflikten (2008–2009) og Gaza-krigen (2014) (Parker et al., 2009; Paret, Craig, & Gilbert, 1986, 790-798). Hvilke kriger som har vært en trussel mot statens eksistens varierer fra kilde til kilde. Enkelte hevder alle, andre hevder ingen etter fredsavtalen med Egypt i 1979.

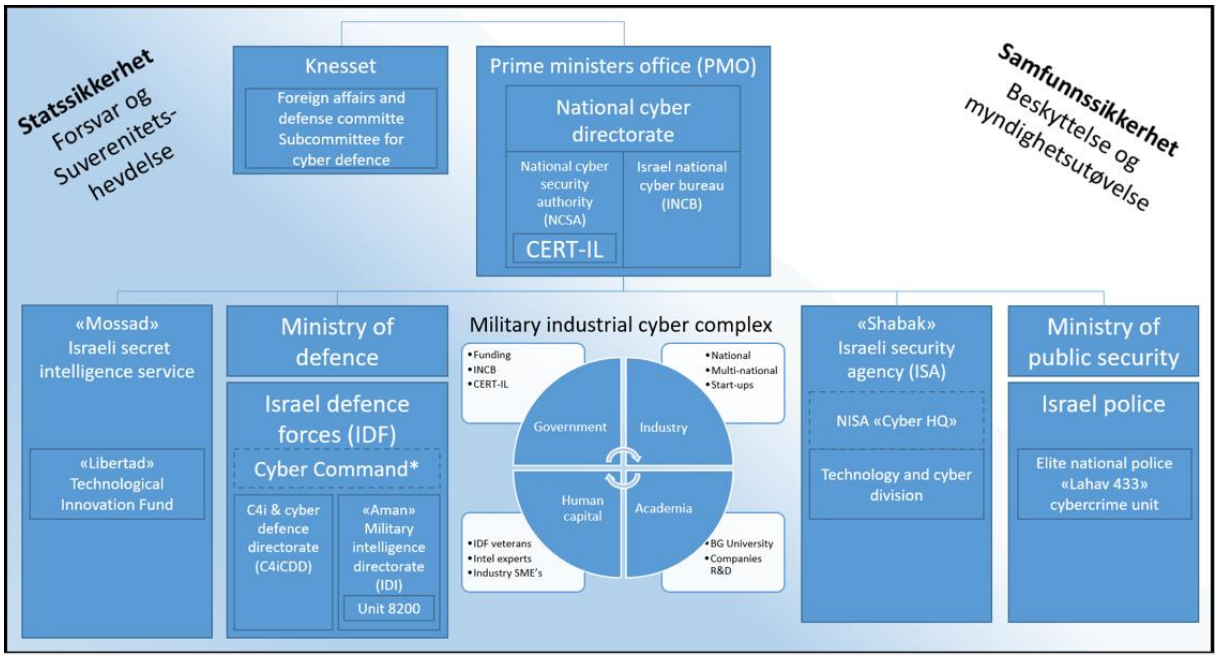
[15] Oversatt fra «operations betweeen wars» og «campaigns between wars», gjerne forkortet OBW og CBW.

I 2014 stod Israel for nesten ti prosent av det globale cybersikkerhetsmarkedet, og eksporterte løsninger for nesten seks milliarder dollar (Tabansky, 2016a, s. 112). Både Norge og Israel er blant verdens mest digitaliserte land med en høyt utdannet befolkning. Digitaliseringen omfatter både samfunnet og militærmakten. Den mest relevante forskjellen for den videre analysen er at Israel karakteriserer seg selv som en cyberstormakt, mens Norge karakteriserer seg selv som digitalt sårbar (se NOU 2015:13; NOU 2016:19; Lysne et al., 2016).

I denne delen skal jeg først sammenligne israelsk og norsk organisering, for deretter å gjøre en komparativ analyse av de to landenes prinsipielle forskjeller i bruk av cybermakt.

2.1 Israelsk forsvar, suverenitetshevdelse og myndighetsutøvelse

Israel har hatt fokus på cybersikkerhet siden 1990-tallet (Tabansky & Ben-Israel, 2015, s. 31-34), men det var først etter at den ambisiøse målsettingen om å være blant de fem største globale cybermaktene ble lagt frem i *National cyber initiative* i 2010 at det etablerte organer for enhetlig ledelse av cybermakt (Housen-Couriel, 2017, s. 8; Tabansky, 2013, s. 81). Figur 1 gir en fremstilling av de mest sentrale organisatoriske elementene i israelsk cybermakt og vil forklares i de neste avsnittene.



Figur 1: Organisering av cybermakt i Israel. *Ikke etablert per mai 2018. (Forfatterens illustrasjon)

2.1.1 Politisk ledelse – Sentralisert myndighet

Etter at Israel bestemte seg for å forfølge målet om cybermakt, utga regjeringen i perioden 2011 til 2015 tre resolusjoner (33rd Government of Israel, 2015a, 2015b; Israeli Government, 2011) for å ivareta:

- Helhetlig nasjonal konsolidering av aktiviteter i cyberdomenet.
- Nasjonal regulering, politisk ledelse og myndighetsutøvelse innen cyberdomenet.
- Nasjonal beredskap for cybersikkerhet.

Gjennom resolusjonene opprettes «National cyber directorate» (heretter cyberdirektoratet) ved statsministerens kontor (heretter PMO). Cyberdirektoratet består av «Israel National cyber bureau» (INCB) og «National cyber security authority» (NCSA).[16]

Israelsk beredskap og krisehåndtering (inkludert cyber kriser) er fordelt til Ministry of Defence (MoD) med «Home front Command» (militær versjon av det norske sivilforsvaret)

[16] I tillegg har Israels nasjonalforsamling, Knesset, en underkomité for cyberforsvar (subcomittee for cyber defence) som sorterer under Utenriks- og forsvarskomitéen (Even, Siman-tov, & Siboni, 2016, s. 1).

og Ministry of public security. I tillegg har NCSA og Israeli security agency viktige oppgaver (Housen-Couriel, 2017, s. 14). Alle med ansvar for krisehåndtering innen sine respektive områder som nærmere beskrevet i de følgende avsnittene.

Cyberdirektoratet – nasjonalstrategisk ledelsesansvar og krisehåndtering

Cyberdirektoratet, som er en organisatorisk enhet i PMO, er ansvarlig for cyberforsvar innen både stats-, samfunns- og individsikkerheten, med INCB og NCSA som utførende myndigheter. NCSA har et ansvar for forsvar av cyberdomenet på tvers av sivile offentlige sektorer og private aktører, og for *samarbeid* med forsvarssektoren.[17] Dette fritar ikke de enkelte sektorer fra ansvaret om egenbeskyttelse[18], men forplikter dem til å følge cyberdirektoratets føringer. For beskyttelse av infrastruktur utover kritiske funksjoner gjelder følgende for Israels del: «only the organization can bear the responsibility for securing itself. On the other hand, a lone organization clearly cannot muster the expertise and resources needed to address the full range of threats …» (Israeli National Cyber Bureau, 2015, s. 2). Under ledelse av cyberdirektoratet har NCSA en rekke oppgaver for å ivareta beredskap og cyberforsvar, herunder trusselanalyser og tidlig varsling, drift av CERT-IL og aktive forsvarsoperasjoner (active defence[19]) (Baram, 2017, s. 6). INCB har ansvaret for å fremme og utvikle nasjonale regulativer for myndighetsutøvelse og lederskap innen nasjonal cybersikkerhet i offentlig og privat sektor. Cyberdirektoratets mest relevante oppgaver for den videre analysen er:

- Forsvare det sivile cyberdomenet og produsere et felles cyber-trusselbilde.
- Forestå offentlig varsling og utvikle samfunnets forståelse og håndtering.
- Fremme cyberindustri, forskning og utvikling i Israel, og utvikle nasjonale utdanningsplaner og internasjonalt samarbeid.

---

[17] Detaljerte beskrivelser av det sivil-militære samarbeidet innen cyberforsvar er sikkerhetsgradert informasjon og ikke tilgjengelig i åpne kilder.

[18] Cyberdirektoratet publiserte i 2017 anbefalte retningslinjer for sivile virksomheters egenbeskyttelse (se Israel National Cyber Security Authority, 2017)

[19] Det er ikke oppgitt i åpne offisielle kilder hva Israel mener med aktivt forsvar, men begrepet er normalt relatert til militære forsvarsoperasjoner som bruker aktive mottiltak for å nøytralisere eller uskadeliggjøre en trussel (se NATO Standardization Agency, 2016).

- Etablere konsept for krisehåndtering og gjennomføre nasjonale og internasjonale øvelser.
- Utarbeide lover og regulativer som ivaretar statens sikkerhet, personvern og demokratiske rettigheter.
- Utvikle samarbeid og koordinering mellom offentlig og privat sektor, med forsvarssektoren samt den akademiske og industrielle sektoren.

Oppsummert har cyberdirektoratet, med INCB og NCSA, et tverrsektorielt ansvar for utvikling og utøvelse av strategisk ledelse, beskyttelse, og myndighetsutøvelse i den sivile delen av det nasjonale cyberdomenet. Cyberdirektoratet har derimot ikke ansvar for forsvar av det militære cyberdomenet eller offensive handlinger rettet mot fremmedstatlige trusselaktører.

2.1.2 Sivile organer – Myndighetsutøvelse og koordinering

CERT-IL – Nasjonalstrategisk respons og koordinering

Det nasjonalstrategiske responsmiljøet, «Cyber event readiness team» (CERT-IL) som ble opprettet i 2015 under ledelse av NCSA i cyberdirektoratet, er en organisatorisk del av PMO, men samlokalisert med det militærindustrielle cyberkomplekset. CERT-IL har et nasjonalt tverrsektorielt ansvar for beskyttelse og forsvar av sivil infrastruktur, og fungerer som kontaktpunkt for både offentlig sektor, private virksomheter og privatpersoner. I 2016 var det fortsatt kun sivil kritisk infrastruktur som var beskyttet av CERT-IL, mens annen sivil infrastruktur utover dette lå ubeskyttet (Tabansky, 2016b, s. 59).[20] Hva som skal beskyttes, reguleres av INCB's styringskomite. Kritisk infrastruktur beskyttet av CERT-IL omfatter blant annet offentlige myndigheter, rettssystemet, fengselssystemene, banker, utvalgt forsvarsindustri, energiselskaper, vannforsyning, sykehus, kommunikasjons- og internett-tilbydere, nasjonale flyselskap, jernbane, havner og børsen (Housen-Couriel, 2017, s. 13).[21]

[20] Status på beskyttelse av sivil infrastruktur i Israel utover kritisk infrastruktur er per mai 2018 ikke tilgjengelig i åpne kilder.

[21] I 2015 ble utviklingen av en sikker plattform for informasjonsdeling mellom CERT-IL og sivile enheter påbegynt (Fishler, 2015).

Uavhengig av hva ulike kilder legger i CERT-ILs aktive forsvarstiltak, forenkles og muliggjøres både proaktive og reaktive mottiltak mot cybertrusler gjennom følgende forhold:

- Organisatorisk nærhet til politisk ledelse.
- Fysisk samlokalisering med både militære og sivile aktører i cyberkomplekset.
- CERT-ILs ansvar for å informere og koordinere med sikkerhets- og forsvarssektoren.

Cybertrusler kan ikke bekjempes eller avvæpnes med cybermakt alene (Libicki, 2016, s. 137), og derfor heller ikke av CERT-IL alene, men Israels organisering åpner for at landet kan velge sine tiltak for forsvar, suverenitetshevdelse og myndighetsutøvelse blant statens samlede maktmidler – det være seg anti-subversjon, tradisjonell militærmakt, politi, diplomati, cyberforsvar eller en kombinasjon av flere maktmidler.

Politiet – Reaktiv myndighetsutøvelse

I 2012 ble det etablert en enhet for cyberkriminalitet i politiets spesialenhet, Lahav 433 (sammenlignbart med det norske Cybercrime-senteret). Enheten spesialiserer seg på digital etterforskning og bevisføring (Housen-Couriel, 2017, s.13). Det fremgår ikke av åpne kilder hvilken rolle enheten har innen nasjonal myndighetsutøvelse, forebygging og bekjempelse i cyberdomenet, men det faktum at politiet ikke er benevnt i regjeringens tre resolusjoner antyder at politiets myndighetsutøvelse er reaktiv og begrenset til etterforskning og påtalemyndighet – og at proaktive tiltak mot interne og eksterne trusselaktører er overlatt til den nasjonale sikkerhetstjenesten «Shabak»[22] og IDF. Politiets reaktive rolle kan forklares med at de fleste cyberangrep rettet mot Israel har sin opprinnelse utenfor staten Israel, og dermed utenfor politiets ansvarsområde.

Den nasjonale sikkerhetstjenesten – Proaktiv myndighetsutøvelse

«Shabak» eller Israeli Security Agency (heretter ISA) rapporterer direkte til PMO og er Israels interne sikkerhetstjeneste (sammenlignbar med Politiets sikkerhetstjeneste i Norge).

[22] Også kjent som Shin Bet.

Etterretning og operasjoner i cyberdomenet er et sentralt element innen alle ansvarsområdene til ISA, og understøttes av sikkerhetstjenestens «Cyber HQ» og «Technology and cyber division». Rundt en fjerdedel av ISAs ansatte er konsentrert rundt cyberteknologi og stordata i forbindelse med tjenestens ansvar for å beskytte statshemmeligheter og kontre cybertrusler, spionasje, terrorisme og subversjon. Ved opprettelsen av cyberdirektoratet og CERT-IL overflyttet man dit deler av ISAs «Cyber HQ», eller «National Information Security Agency», ansvar for beskyttelse av kritisk infrastruktur (Housen-Couriel, 2017, s. 13). Begrunnelsen var blant annet å etablere nødvendig koordinering og samarbeid, samt mobilisering av nasjonale innsatsfaktorer (Israeli National Cyber Bureau, 2015, s. 3). Anti-subversjonsvirksomheten er sentral for å forebygge og bekjempe terror og har siden den elektroniske intifadaen[23] i økende grad blitt rettet mot cyberdomenet (se Yin, 2009). ISA kan ikke overvåke israelske borgere i Israel uten særskilt tillatelse (Lapid & Gilboa, 2012), men kan gjennomføre målrettet cyberetterretning, pågripelser og avhør. Selv om ISA er en innenriks sikkerhetstjeneste, har de siden Seksdagerskrigen i 1967 hatt ansvaret for etterretning og operasjoner (med både menneskelige og teknologiske ressurser) i de palestinske selvstyreområdene (Vestbredden og Gazastripen) og Golanhøydene.

Aktiviteter utenfor Israel og selvstyreområdene koordineres med de øvrige etterretningstjenestene: Mossad og IDFs Military Intelligence Directorate (heretter IDI). Nærmere samarbeid med de militære styrkene på taktisk, operasjonelt og strategisk nivå ble spesielt aktualisert etter at etterretningsutfordringer ble identifisert som en av årsakene til mangelen på suksess i krigen mot Hizbollahs hybride krigføring i 2006 (Hoffman, 2007, s. 35-55; Lapid & Gilboa, 2012). ISA ble for eksempel integrert i militære feltenheter og hovedkvarter på alle nivå i Gaza-konflikten i 2008-2009 for å bidra med sin ekspertise innen både tradisjonelle etterretningsdisipliner og digital etterretning mot asymmetriske motstandere (Lapid & Gilboa, 2012).

ISA understøtter statssikkerheten ved å støtte de militære styrkenes forsvar og suverenitetshevdelse med etterretninger og operasjoner, både i og utenfor cyberdomenet. ISAs

[23] «The Electronic intifada» er betegnelsen på den palestinske on-line motstandskampen som startet samtidig med den Andre intifada i 2000. Den elektroniske intifadaen søkte å påvirke USA, EU og internasjonale organisasjoner med budskap om Israel som okkupant, ulovlige bosettinger og brudd på menneskerettigheter.

arbeid på cyberområdet for kontraetterretning, kontraterror og anti-subversjon konsentrerer seg i hovedsak om ivaretakelse av samfunnssikkerheten, gjennom myndighetsutøvelse innenfor sine avgrensede ansvarsområder og innenfor israelsk lov. Juridisk står ISAs oppdrag om myndighetsutøvelse overfor samme demokratiske dilemma som Etterretningstjenesten og PST i Norge: digital masseovervåkning utfordrer personvernet og demokratiske rettigheter, og er forbudt ved lov. Israelsk praksis tillater likevel hyppigere statlige inngripen overfor personer enn i Norge, selv om loven forbyr masseovervåkning av israelske borgere i Israel (Cate & Dempsey, 2017, s. 26-97; Lapid & Gilboa, 2012). ISA kan likevel agere på informasjon fra andre instanser, som CERT-IL.

2.1.3 Militære enheter – Forsvar og suverenitetshevdelse

IDFs Cyberkommando – Militærstrategisk ledelse?

Israelske myndigheter besluttet i 2015 at enhetene med ansvar for utøvelse av defensive og offensive cyberoperasjoner skulle organiseres under én militærstrategisk ledelse, «IDF cyber command», og sidestilles med land-, luft- og sjøstridskreftenes kommandoledd. Det ble samtidig annonsert at cyberkommandoen skulle samlokaliseres med private og offentlige cyberaktører i Israels militærindustrielle cyberkompleks. Beslutningene har ifølge åpne kilder møtt stor motstand fra etterretningstjenestene (IHS Jane's, 2017; Israeldefense, 2017; Magid, 2017) og er per mai 2018 ikke effektuert, men er heller ikke offentlig kansellert av israelske myndigheter.

Basert på IDFs strategi (hvor cyberoperasjoner utgjør en betydelig kapasitet innen den militære maktanvendelsen), det nasjonale krisehåndteringssystemet, og empiri fra tidligere kriger og profilerte cyberoperasjoner, er det sannsynlig at cyberoperasjoner *i krig* ledes av generalstaben. Det er videre sannsynlig at også cyberoperasjoner med begrensede *militære målsettinger* mellom kriger ledes av generalstaben, mens cyberoperasjoner med *politiske målsettinger* mellom kriger (for eksempel operasjon Olympic games som hadde potensielt politiske og strategiske følgekonsekvenser) ledes direkte fra PMO. Sannsynligheten underbygges av at både israelsk politikk og militær strategi dyrker nytenkning, initiativ, handlekraft og besluttsomhet på lavest mulig nivå, og søker å unngå over-regulering og tunge

beslutningsprosesser (Israeli Defence Forces, 2016, s. 32-33; Netanyahu, 2016). Ansvaret for gjennomføring av offensive og defensive operasjoner ligger i dag delt på den militære etterretningstjenesten og «C4i[24] and cyber defence directorate» (heretter C4iCDD). En av årsakene til at Israel fortsatt ikke har etablert en militær cyberkommando som tidligere besluttet, kan være at landets demonstrerte suksess med bruk av cybermakt hittil ikke har påkalt et omorganiseringsbehov. Tvert imot: forsvar og suverenitetshevdelse med gjeldende organisering av cybermakten har understøttet statssikkerheten.

IDFs C4i and Cyber Defence Directorate – Cyberforsvar og avgrenset myndighetsutøvelse

IDF har alltid fokusert på kvalitativ overlegenhet, og omfavnet på 1990-tallet en USA-inspirert doktrine for effektbasert operasjoner (EBO), hvor høyteknologiske løsninger innen luftmakt, presisjonsstyrte våpen og informasjonsoverlegenhet stod sentralt (Matthews, 2008, s. 23-28). Digitalisert og høyteknologisk kampkraft har ført med seg nye muligheter, men også nye sårbarheter som må forsvares.

C4iCDD har ansvaret for å beskytte og forsvare de væpnede styrkene og resten av forsvarssektoren mot cybertrusler og angrep.[25] Enheten gjennomfører jevnlig øvelser innen EK og cyberforsvar, og arrangerer såkalte «hackatons» med både sivile og internasjonale deltakere (Opall-Rome, 2017). C4iCDD tar inn en stort antall vernepliktige soldater som spesialiseres innen cyberforsvar og sikkerhet. C4iCDD styrkeproduserer målrettet fageksperter, gründere og ledere til det militærindustrielle cyberkomplekset som en del av en langsiktig strategi.

I 2016 ble det besluttet at C4iCDD også skal ha et ansvar for motangrep og aktivt forsvar, samt forsvar av utvalgt sivil kritisk infrastruktur i krisesituasjoner (Gross, 2017; Israeldefense, 2017). Dette er ikke bekreftet i offentlige kilder, men med bakgrunn i at Israels definisjon av forsvar er proaktiv og offensivt rettet, og at C4iCDD har egne enheter trent for offensive operasjoner (Opall-Rome, 2017), er det ikke usannsynlig at dette er tilfelle. Det er likevel lite sannsynlig at C4ICDD vil være i stand til å gjennomføre offensive operasjoner for å oppnå

[24] Command, control, communication, computer and intelligence

[25] Sammenlignbar med Cyberforsvaret i Norge

strategiske målsettinger, men sannsynlig at de kan gjennomføre operasjoner med begrenset effekt for å oppnå operasjonelle og taktiske målsettinger. En slik kapasitet vil være på linje USAs konsept for taktiske cyberoperasjoner (se for eksempel Porche III et al., 2017) og med Israels cyberstormaktambisjon. C4IDDs ansvar for beskyttelse og forsvar av sivil kritisk infrastruktur i krise og krig er blitt fremhevet som vanskelig å gjennomføre i praksis. Dette begrunnes med at IDF må være til stede kontinuerlig for å gjøre seg kjent med infrastrukturen, dens styrker og sårbarheter, for å kunne utøve effektivt forsvar (Even et al., 2016, s. 3).

Gitt C4iDDs oppdrag om aktivt cyberforsvar, inkludert offensive mottiltak, bidrar C4iCDD til suverenitetshevdelse på to måter. For det første bidrar beskyttelse og forsvar av de israelske land-, luft- og sjøstyrkenes høyteknologiske kampplattformer og ledelsessystemer mot fiendtlig EK og digitale operasjoner, til å bevare statens evne til forsvar og suverenitetshevdelse. For det andre ved at aktivt forsvar kombinert med offensive cyberoperasjoner kan bidra til å avskjære, forhindre og avskrekke fremmedstatlig etterretning, sabotasje og påvirkning. Det siste poenget vil riktig nok kun ha begrenset og midlertidig effekt på en fremmedstatlig kompetent motstander, og må nødvendigvis kombineres med andre maktmidler for å ha varig effekt, fordi man ikke kan avvæpne motstandere i cyberdomenet alene.

IDIs Unit 8200 – Cyberkrigføring og tidlig varsling

«Aman» eller «IDF Intelligence Directorate» (heretter IDI) er Israels militære etterretningstjeneste (sammenlignbar med Etterretningstjenesten i Norge), og er den største etterretningsenheten i Israel. IDI er direkte underlagt generalstaben, men har også rapporteringsansvar direkte til PMO, hvor tjenestens sjef har et særskilt ansvar for å støtte politiske myndigheter med nasjonale etterretnings- og trusselvurderinger og rådgivning om sikkerhets- og utenrikspolitiske forhold. IDI har ansvaret for utenriks etterretning i Israels nærområder og for offensive cyberoperasjoner. Men IDFs viktigste oppdrag er tidlig varsling av trusler, angrep og fiendtlige aktiviteter som kan true statssikkerheten, inkludert cyberangrep.

Enheten for cyberkrigføring, Unit 8200, er IDIs største enhet. Enheten skal bestå av rundt 10000 yrkesoffiserer, reservister og vernepliktige soldater og har erfaring fra arbeid med elektronisk krigføring og signaletterretning fra Israels opprettelse i 1948. Enheten har i dag ansvar for både cyberetterretning, dekryptering, og offensive cyberoperasjoner (Baram, 2017; IDF, 2018). Unit 8200 er kjent som en av verdens mest avanserte enheter for cyberkrigføring og for å ha stått bak noen av historiens mest omfattende og avanserte cyberoperasjoner, blant annet Stuxnet-ormen som saboterte Irans uran-anrikningsprogram. Svært mange av enhetens soldater går etter endt tjeneste inn som fageksperter i Israels militærindustrielle cyberkompleks.

Unit 8200s mest omtalte cyberoperasjoner går utover begrepet suverenitetshevdelse og har proaktivt søkt å forhindre at Iran og Syria erverver atomvåpen ved hjelp av offensiv cybermakt. Med andre ord ikke *suverenitetshevdelse i cyberdomenet*, men *forkjøpsangrep gjennom cyberdomenet*, med både fysiske og kognitive effekter i de øvrige domenene. Cyberoperasjoner for å hevde israelsk suverenitet ved å avskjære eller hindre offensive cyberangrep mot staten er lite omtalt. Men selv om cybermakt ikke kan nøytralisere eller uskadeliggjøre cybertrusler alene, utgjør suverenitetshevdelse sannsynligvis en betydelig del av den proaktive innsatsen til Unit 8200 i samvirke med statens øvrige maktmidler. Enhetens viktigste bidrag til statssikkerheten er den høyteknologiske kapasiteten innen etterretning i og gjennom cyberdomenet. Den betydelige høyteknologiske etterretningskapasiteten som Unit 8200 besitter, er for Israel en kompensasjon for mangel på strategisk dybde og muliggjør tidlig varsling; en forutsetning for statens forsvar, suverenitetshevdelse, og myndighetsutøvelse både i og utenfor cyberdomenet. Hvordan Unit 8200 bidrar til israelsk cybermakt, utdypes i kapittel 3.1.3.

Mossad – Spesielle operasjoner utover forsvar og suverentitshevdelse

Mossad er ikke en uniformert militær enhet, men består i hovedsak av offiserer og IDF-veteraner, og jobber som en integrert del av IDFs militære operasjoner. Mossad er direkte underlagt PMO, og har koordineringsansvar for aktiviteter og operasjoner utenlands overfor de øvrige etterretningsorganene IDI og ISA. Mossad gjennomfører operasjoner i hele verden, mens IDF har fokus på Israels nærområder.Mossad har et proaktivt ansvar for å hindre

terrorangrep og stoppe trusler fra masseødeleggelses- og ukonvensjonelle våpen. Ansvaret utelukker ikke cybertrusler. Mossad har tidligere fokusert hovedsakelig på spesielle operasjoner med menneskebaserte innhentingsmetoder (HUMINT) og operatører. I senere tid har fokuset på cyberoperasjoner økt. Blant annet skal det ha vært sentralt i Operasjon Orchard i 2007, med både HUMINT, EK og inntrengning i datasystemer (Singer & Friedmann, 2014, s. 126-128). Mossads operasjoner er det naturlig nok lite åpenhet rundt, men det skal blant annet ha etablert en egen enhet for cyberkrigføring (Silverstein, 2016), og har et eget sponsorsprogram rettet mot det militærindustrielle cyberkomplekset. Programmet skal understøtte Mossads operasjoner med blant annet robotisering, kryptologi og analyse av stordata (Mossad, 2017).

Mossads operasjoner utenriks strekker seg utover det vi normalt regner som forsvar og suverenitetshevdelse. Enheten bruker ukonvensjonelle midler og spesielle operasjoner, inkludert cybermakt, for proaktivt å hindre eller stoppe andre stater *før* de utvikler teknologi eller evner som kan true Israels eksistens.

2.1.4 Sivilmilitært samarbeid – Det militærindustrielle cyberkomplekset

Israel har satt seg en høy målsetting om å bli en ledende cyberstormakt og inviterer andre nasjoner med sammenfallende interesser til cybersikkerhetssamarbeidet. Det har invitert, og på svært kort tid, etablert et industrielt, økonomisk, vitenskapelig og militært kompleks, hvor nasjonale og internasjonale aktører bidrar. Her samles de største IT-gigantene i verden, sammen med et stort antall israelske gründere innen cybersikkerhet, akademia og forskningsmiljøer, myndighetene, forsvaret og etterretningstjenestene. Rundt 10 000 veteraner fra C4iCDD og Unit 8200 utgjør navet i dette komplekset som i dag er spydspissen i israelsk økonomisk vekst. IDF forventes å styrkeprodusere 2000 – 3000 spesialister innen cyberfaget årlig til cyberkomplekset (Cyberspark, 2018). Hvordan dette militærindustrielle cyberkomplekset bidrar til israelsk cybermakt, utdypes i kapittel 3.1.2.

2.2 Norsk forsvar, suverenitetshevdelse og myndighetsutøvelse

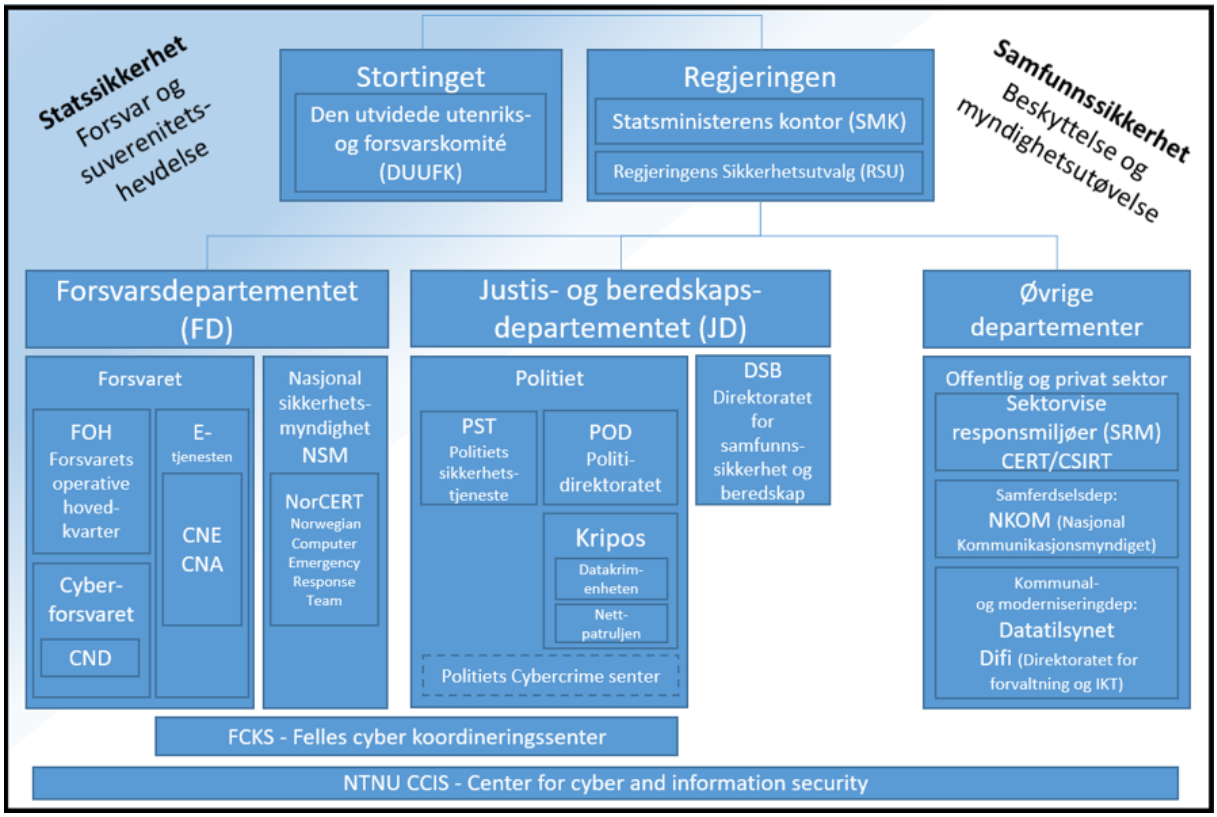
I Norge finnes det ingen enhetlig overordnet politisk ambisjon om cybermakt, men Norge har lang tradisjon med organisering av ansvar for ivaretakelse av informasjonssikkerhet.[26] Sammenlignet med Israels Cyberdirektorat ved PMO har ikke Norge *ett* konstitusjonelt politisk organ som har ansvaret for cyberforsvar og cybersikkerhet tilknyttet Statsministerens kontor (SMK); ansvaret er fordelt på alle departementer og underliggende direktorater som har tverrdepartementale oppgaver og nasjonalt ansvar.

De norske prinsippene for krisehåndtering: *ansvar, likhet, nærhet og samhandling* er styrende for den norske organiseringen for utvikling og håndtering av beredskap og krisehåndtering (Samfunnssikkerhetsinstruksen, 2017). Prinsippene gjelder også for regjeringens handlingsplan for informasjonssikkerhet, og dermed også cybersikkerhet og organiseringen av cybermakt (Kommunal- og moderniseringsdepartementet, 2015, s. 8). *Ansvarsprinsippet* innebærer at alle sektorer har ansvar for håndtering av egen sikkerhet, inkludert cybersikkerhet. *Likhetsprinsippet* innebærer lik organisering og ansvarsfordeling i fred, krise og krig. *Nærhetsprinsippet* innebærer at kriser håndteres på lavest mulig nivå.[27] Det siste prinsippet er *Samhandlingsprinsippet*[28] og innebærer at den enkelte sektor har selvstendig ansvar for å samhandle med alle andre sektorer, virksomheter og aktører i forebygging, beredskap og krisehåndtering (Justis- og beredskapsdepartementet, 2012, s. 39). Figur 2 gir en fremstilling av de mest sentrale organisatoriske enhetene i norsk cybermakt.

[26] Norges nasjonale strategi for informasjonssikkerhet ble første gang utgitt i 2003 (Regjeringen Bondevik II, 2003) og siste fornyet i 2012 (Departementene, 2012).

[27] Med unntak av sikkerhetspolitiske kriser: "Sikkerhetspolitiske kriser og atomulykker vil på grunn av sin karakter alltid kreve en overordnet styring og koordinering fra sentralt myndighetsnivå, men vil like fullt kunne medføre iverksetting av tiltak og håndtering på alle forvaltningsnivåer.» (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015, s. 17).

[28] Samhandlingsprinsippet ble tatt frem i kjølvannet av hendelsene 22. juli 2011 og etter gjentatt kritikk av ansvarsprinsippet (alle har ansvaret fører i praksis til at ingen har ansvaret).



Figur 2: Organisering av cybermakt i Norge. (Forfatterens illustrasjon)

2.2.1 Politisk ledelse – Ansvarsprinsippet

I tråd med de norske prinsippene er det regjeringen som har det øverste ansvar for å håndtere nasjonal sikkerhet og beredskap, inkludert håndtering av alvorlige cyberhendelser. Stortinget har ingen spesifikk kommisjon for cyberrelaterte saker, men saker relatert til forsvar og suverenitetshevdelse vil naturlig havne i Utenriks- og forsvarskomiteen eller Den utvidede utenriks- og forsvarskomiteen (DUUFK). Justis- og beredskapsdepartementet (JD) er fast lederdepartement ved kriser i fredstid, med mindre annet er bestemt. I krig, eller hvis norsk suverenitet trues og krisen blir sikkerhetspolitisk, er Forsvarsdepartementet (FD) lederdepartement.[29] Kriserådet (KR) er et administrativt organ opprettet for å styrke den

[29] Regjeringens sikkerhetsutvalg (RSU) ledes av statsministeren og består normalt av utenriksministeren, justisministeren, forsvarsministeren og finansministeren. RSU behandler sensitive saker av forsvars- og

strategiske koordineringen i alle typer kriser til støtte for regjeringen, SMK og gjeldende lederdepartement. Krisestøtteenheten (KSE) er organisatorisk underlagt JD og er til støtte for KR og det til enhver tid gjeldende lederdepartement.[30] På militær side støttes FD av et eget situasjonssenter ved kriser, og Utenriksdepartementet (UD) har et operativt senter til understøttelse. Disse samarbeider med KSE når det er relevant (Direktoratet for samfunnssikkerhet og beredskap, 2015, s. 14).

Hovedansvaret for utvikling av cybersikkerhet og håndtering av hendelser i cyberdomenet er i hovedsak fordelt på to departementer: JD og FD. JD har siden 2013 hatt samordningsansvaret for forebyggende IKT-sikkerhet på sivil side[31], mens FD har ansvaret for IKT- og cybersikkerhet i militær sektor.[32] De neste avsnittene vil forklare departementene og deres underliggende organers bidrag til utvikling og hevdelse av norsk cybermakt.

2.2.2 Sivile organer – Koordinering og myndighetsutøvelse

Nasjonal Sikkerhetsmyndighet

NSM er et sivilt direktorat underlagt FD med et sektorovergripende ansvar for forebyggende sikkerhet i Norge, og med rapporteringsplikt innen sitt samfunnsoppdrag til JD. NSMs myndighet begrenser seg til oppfølging av sikkerhetsloven for å beskytte nasjonale sikkerhetsinteresser og landets «suverenitet, territorielle integritet og demokratiske styreform» (Forsvarsdepartementet, 2016b, s. 7). Virksomheter, objekter, infrastruktur eller funksjoner

---

sikkerhetspolitisk betydning. Alvorlige og omfattende cyberhendelser, som fremmedstatlig digital etterretning og sabotasje, kan være i denne kategorien.

[30] KSE bemanner et sivilt situasjonssenter med døgnkontinuerlig beredskap, som skal holde en oppdatert situasjonsforståelse basert på innspill fra en rekke aktører, herunder Nasjonal Sikkerhetsmyndighet (NSM), og rådgi KSE og lederdepartementet i strategisk krisehåndtering.

[31] Ansvaret for samordning av forebyggende IKT-sikkerhet i sivil sektor ble overført fra Fornyings-, administrasjons- og kirkedepartementet til JD, med virkning fra 1. april 2013 (Statsministerens kontor, 2013)

[32] I tillegg har Samferdselsdepartementet (SD), Kommunal- og moderniseringsdepartementet (KMD), Kunnskapsdepartementet (KD) og UD sentrale roller for en helhetlig ivaretakelse av en nasjonal cyberpolitikk og myndighetsutøvelse gjennom underliggende direktorater.

utenfor statsforvaltningen som ikke behandler gradert informasjon, for eksempel industrielle styringssystemer for olje- og gassutvinning, eller logistikk og forsyninger til Forsvaret, omfattes ikke automatisk av sikkerhetsloven. Ny sikkerhetslov[33] tar sikte på å sikre *grunnleggende nasjonale funksjoner*[34] og gir NSM et bredere myndighetsansvar for å bidra til norsk suverenitet: «Med [grunnleggende nasjonale funksjoner] menes tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.» (Forsvarsdepartementet, 2016b, s. 7).[35] NSM leder Felles cyber koordineringssenter (FCKS) og er i tillegg ansvarlig for å drifte Norwegian Computer Emergency Response Team (NSM NorCERT) omtalt i de neste avsnittene.

NSM NorCERT – Nasjonalstrategisk monitorering, deteksjon, varsling og koordinering

NSM NorCERT er en sivil enhet i NSM, og har et nasjonalt sektorovergripende ansvar for monitorering og koordinering av cyberhendelser. Ansvaret innebærer varsling, rådgiving og støtte overfor den enkelte sektor eller virksomhet som selv er ansvarlig for håndteringen av cybertrusler og angrep (Sikkerhetsloven, 1998, § 9 e og f).

Et nasjonalt system for deteksjon av cybertrusler og -angrep, Varslingssystem for digital infrastruktur (VDI), ble opprettet som et prøveprosjekt i år 2000 og innlemmet i NSM NorCERT i 2006. NSM NorCERT beskriver VDI som «en digital innbruddsalarm for AS Norge» (NSM, 2014). Systemet er i dag basert på frivillighet, og er et tilbud til eiere av kritisk infrastruktur om støtte til monitorering og håndtering fra NSM NorCERT. Medlemmer av VDI får utplassert digitale sensorer i sine systemer som monitorer og detekterer anomali basert på signaturer og mønstre fra kjente trusler (Mørkestøl, 2014, s. 96; NSM, 2014). Systemet tilbyr ikke forsvars- eller beskyttelsesfunksjoner i seg selv, men kan oppdage

---

[33] Ny lov ble vedtatt av Stortinget 17. januar 2018, jf. Prop. 153 L (2016-2017), Innst. 103 L (2017-2018), Lovvedtak 27 (2017-2018).

[34] Grunnleggende nasjonale funksjoner omfatter: styringsevne og suverenitet, befolkningens sikkerhet og samfunnets funksjonalitet. Se rapporten *Samfunnets kritiske funksjoner* (Direktoratet for samfunnssikkerhet og beredskap, 2016) for en detaljert beskrivelse av kritiske funksjoner og kritisk infrastruktur.

[35] I dag må slike grunnleggende nasjonale funksjoner hjemles i kongelig resolusjon (Sikkerhetsloven, 1998, § 2 a og b) for å omfattes av sikkerhetsloven – i ny sikkerhetslov vil fagdepartementene selv kunne avgjøre hva som er nasjonens grunnleggende funksjoner (Forsvarsdepartementet, 2016b, s. 8).

digitale angrep, spionasje og forberedelser til sabotasje – noe som er en forutsetning for iverksettelse av ekstra beskyttelsestiltak, gjenoppretting, cyberforsvar, etterforskning og eventuelle offensive mottiltak.

VDI er ikke et system for tidlig varsling, men NSM NorCERTs samarbeid og informasjonsdeling med alle nasjonale sektorer, NATO og andre nasjoner[36] muliggjør likevel at varsler om alvorlige trusler og sårbarheter kan distribueres raskt. Likevel: denne modellen, basert på ansvarsprinsippet, og såkalte multistakeholder initiativer, er beskrives av NUPI-forskeren Lilly Pijnenburg Muller (2016, s. 16-17) i artikkelen *Makt og avmakt i cyberspace* som dysfunksjonell og en av grunnene til norsk avmakt fordi offentlig og privat sektor har motstridende målsettinger og avstår fra å dele informasjon. Ny sikkerhetslov pålegger ikke private aktører som er forvaltere av grunnleggende nasjonale funksjoner eller kritisk infrastruktur å tilknytte seg til VDI (Forsvarsdepartementet, 2016b, s. 44).

NSM NorCERT og VDI «kan behandle personopplysninger i ulike former når det er nødvendig» (Forsvarsdepartementet, 2016b, s. 54)[37]. Selv om VDI ikke kan sammenlignes med et digitalt grenseforsvar (DGF) på grunn av VDIs avgrensede mandat[38], står NSM NorCERT ikke overfor det samme juridiske og demokratiske dilemma som de øvrige etterretnings-, overvåkings- og sikkerhetstjenestene i Norge og Israel, og muliggjør derfor en viss sivil nasjonal cybersituasjonsforståelse. NSM NorCERT deler sin cybersituasjonsforståelse med politidirektoratet (POD) og Forvarets operative hovedkvarter (FOH).

---

[36] NSM NorCERT har også samarbeid blant annet med NATOs responsmiljø. Både NSM NorCERT og Israels CERT-IL er med i det internasjonale FIRST-samarbeidet for deling av teknisk informasjon, verktøy, metoder og prosesser (Se https://www.first.org/members/teams/).

[37] Videreføring av tidligere bestemmelse i Lov om forebyggende sikkerhet. Innebærer: «a) metadata om IKT-trafikk til og fra virksomheter som er knyttet til det nasjonale varslingssystemet for digital infrastruktur b) informasjon som er nødvendig for å analysere utløste alarmer i varslingssystemet c) IP-adresser mottatt fra nasjonale og internasjonale samarbeidspartnere d) logger og infisert maskinvare, etter samtykke fra en virksomhet der dette er nødvendig i forbindelse med bistand til håndtering av alvorlige dataangrep.» (Sikkerhetsloven, 1998, § 10 a)

[38] VDI får kun informasjon fra deltakerne, mens DGF vil se alle relevante trusler mot Norge – ikke bare de som treffer VDI-medlemmene.

Selv om NSM NorCERT ikke har ansvaret for å håndtere cyberhendelser, er det likevel en bidragsyter til både forsvar, suverenitet og myndighetsutøvelse. For det første: digital sabotasje av kritisk infrastruktur eller sektorovergripende cyberkriser kan være en viktig militær og sikkerhetspolitisk indikator om opptakten til konflikt eller forestående kriser og muliggjøre militære forberedelser og respons. For det andre: avdekking av digital spionasje styrker politiets evne til kontraetterretningsarbeid. For det tredje: den enkelte sektors forutsetninger for å redusere sårbarheter og håndtere cyberangrep mot kritiske samfunnsfunksjoner styrkes. Avslutningsvis må det nevnes at det er langt fra alle kritiske samfunnsfunksjoner som er omfattet av NSM NorCERTs VDI (se NOU 2015:13), og at «AS Norge ikke har alarm på alle dører og vinduer» (Gustavsen, 2015, s. 68).

Sektorvise responsmiljøer – Sektorvis håndtering, varsling og koordinering

Den enkelte offentlige og private sektor er i tråd med krisehåndteringsprinsippene ansvarlig for å beskytte seg selv – ikke bare mot kriminell virksomhet (for eksempel med tyverialarmer og vektere), men også mot fremmedstatlig digital etterretning, sabotasje og subversjon. Den enkelte sektor er pålagt å ha sitt eget responsmiljø (Justis- og beredskapsdepartementet, 2012, s. 104), omtalt som Sektorvise responsmiljø (SRM) i *Rammeverk for håndtering av IKT-sikkerhetshendelser,* for å håndtere dette ansvaret. SRM forestår varsling og koordinering i egen sektor, mot andre sektorer og mot NSM NorCERT (Nasjonal Sikkerhetsmyndighet, 2017, s. 11). Beskyttelse må ivaretas av virksomhetene innad i sektoren, og «den enkelte virksomhet som forvalter kritisk infrastruktur og/eller kritiske samfunnsfunksjoner skal … gjenopprette sikker tilstand for berørte systemer, utføre skadevurdering og begrense følgeskader for andre IKT-systemer» (ibid, s. 2).

Politiet – reaktiv myndighetsutøvelse

Myndighetsutøvelse er i hovedsak en oppgave for politiet og sivile myndigheter. Politiets oppgaver strekker seg fra forebygging, bekjempelse og etterforskning av «normal» kriminalitet til spionasje, terrorisme, masseødeleggelsesvåpen og sabotasje.
Politiets sikkerhetstjeneste (PST) er direkte underlagt JD og skal primært forebygge og etterforske ulovlig etterretningsvirksomhet og kriminalitet mot statssikkerheten. Ansvaret

utelukker ikke forebygging av digital spionasje og sabotasje. PST samarbeider med E-tjenesten og NSM i FCKS på dette området.

Kripos er underlagt POD og JD og skal bekjempe organisert og alvorlig kriminalitet. Datakrimenheten i Kripos er spesialisert innen datatekniske undersøkelser, kommunikasjonskontroll og etterforskning av spor på internett, og er politiets kontaktpunkt for internasjonalt operativt samarbeid (Politiet, 2018). Kripos deltar også i FCKS. Politiet har ikke offensive eller defensive cyberkapabiliteter, men kan foreta målrettet etterforskning, ransakelser og pågripelser.[39]

Politiet kan iverksette dataavlesning[40] som et ledd i etterforskning i en tidsbegrenset periode (Politiloven, 1995, § 17 d; Straffeprosessloven, 1981, § 216 o og p), men iverksettelse av dataavlesning krever skjellig grunn til mistanke om kriminalitet, og overvåkningen kan kun rettes mot tjenester som en mistenkt aktør ventes å bruke (Gloppen, 2016, s 19-20, 31). Politiet kan med andre ord ikke foreta varig overvåkning av kritisk infrastruktur for å forebygge og bekjempe digital spionasje, sabotasje eller subversjon.

Politiets myndighetsutøvelse i cyberdomenet er i hovedsak reaktiv, og politiet fremholder selv at det har utfordringer med å ivareta sitt myndighetsansvar innen etterforskning og forebygging med bakgrunn i utdatert lovverk, den voksende IKT-trusselen og at bare 9 % av cyberangrepene anmeldes (Politidirektoratet, 2017, s. 26-30). Fordi cyberangrep ofte har opprinnelse utenfor Norge, er det avgjørende for å kunne bekjempe cybertrusler mot norske interesser at politiet samarbeider med internasjonale organer og andre lands politimyndigheter og sikkerhets- og etterretningstjenester, inkludert Interpol og Europols EC3[41] (Se for eksempel Storruste et al., 2012). Politiets datakrim-strategi fremholder likevel at fremmedstatlige digitale operasjoner ikke kan bekjempes med internasjonalt politisamarbeid alene (Politidirektoratet, 2015, s. 81-82). Trusselaktører utenfor Norge vil måtte håndteres med en kombinasjon av juridiske, politiske, diplomatiske og i ytterste konsekvens militære

[39] Politiets Cybercrime-senter startet etableringen i 2018 (Trædal, 2017), men vil uten en endring i lovgivningen være reaktivt rettet, med en forebyggende rolle begrenset til etterforskning.

[40] Dataavlesning kan for eksempel gjøres ved hjelp av skjult avlesningsutstyr eller inntrengning og installasjon av spionprogramvare. Dataavlesing er utredet i kapittel 23 i NOU 2009: 15 Skjult informasjon – åpen kontroll.

[41] Europeisk datakrimsenter.

maktmidler. Det er i det hele lite som tyder på at politiet er i stand til helhetlig myndighetsutøvelse i cyberdomenet.

Sivil offentlig sektor – Myndighetsutøvelse

Nasjonal kommunikasjonsmyndighet (Nkom) er underlagt Samferdselsdepartementet og har ansvaret for å forvalte ekomloven. Nkom har videre et ansvar for koordinering og rapportering ved uønskede hendelser som rammer ekomnett og for frekvensforvaltning. Nkom arbeider også med forebyggende IKT-sikkerhet nasjonalt. Nkom kan pålegge offentlige og private aktører å sette i verk tiltak for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i elektronisk kommunikasjonsnett. Nkom opprettet i 2015 en egen responscelle for ekom-sektoren, Nkom CSIRT. Nkom er eneste myndighet som kan å stenge ned internett og radiotjenester dersom det er aktuelt for å isolere eller redusere omfanget av elektromagnetiske forstyrrelser eller spredning av skadevare (NOU 2015:13, s. 102-106).

KMD har ansvaret for å koordinere regjeringens IKT-politikk og personvernpolitikk. Datatilsynet og Direktoratet for forvaltning og IKT (Difi) er underlagt KMD. Datatilsynet kontrollerer at personopplysninger blir behandlet i samsvar med lov og forskrift. Mens politiet og E-tjenesten har rettsregler for å kunne innhente nødvendig informasjon, har private aktører kun avtalen med forbruker som ramme og heller ikke samme krav for å beskytte informasjonen som kan være av verdi for fremmedstatlig etterretning. Difi arbeider for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i offentlig forvaltning og er rådgivende organ for utforming av IKT-politikken. DSB ligger under JD og har et ansvar for nasjonal sikkerhet og beredskap på sivil side. Ansvaret innebærer etatsstyring av Sivilforsvaret og drift av kritisk telekommunikasjonsinfrastruktur for nød- og beredskapsaktører. DSB har ikke et særskilt ansvar for cybersikkerhet som en del av det nasjonale sikkerhets- og beredskapsarbeidet, det tilligger NSM.

Siden cybermakt er avhengig av teknologien som muliggjør operasjoner i cyberdomenet, er SD og KMD med Nkom, Datatilsynet og Difi viktige aktører for å utøve myndighet i cyberdomenet.

2.2.3 Militære enheter – Forsvar og suverenitetshevdelse

Forsvarets operative hovedkvarter – Fellesoperativ ledelse

Statssikkerhet ivaretas i Norge av Forsvaret. Forsvarets fremste oppgave er å «forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar» (Forsvarsdepartementet, 2016c, s. 23). Sjef Forsvarets operative hovedkvarter (FOH) utøver kommando over norske styrker og sikrer norske interesser ved å planlegge og lede militære fellesoperasjoner i fred, krise og krig – nasjonalt og internasjonalt. FOH's fremste oppgave i daglige fredstidsoperasjoner er suverenitetshevdelse – i sjødomenet ved hjelp av Marinen og Kystvakten, i luftdomenet med Luftforsvarets F-16 beredskap, og i landdomenet med Grensevakten og styrker på beredskap. Forsvaret er ikke gitt eksplisitt oppdrag om å utøve suverenitet i cyberdomenet, og det er regjeringen som avgjør om et cyberangrep er å anse som et brudd på norsk suverenitet.

FD oppgir at «Cyberangrep som del av væpnet konflikt skal håndteres som del av FDs konstitusjonelle ansvar.» (Forsvarsdepartementet, 2014, s. 11). Forsvaret er i tillegg ansvarlig for myndighetsutøvelse på utvalgte områder hvor politiet og sivile myndigheter ikke har egnede kapasiteter men Forsvaret av hensyn til sitt oppdrag om forsvar og suverenitet må være til stede. Forsvaret er ikke gitt eksplisitt oppdrag om begrenset myndighetsutøvelse i cyberdomenet, men FOH beslutter om Forsvaret skal yte bistand til politiet og sivilsamfunnet, inkludert bistand ved alvorlige cyberangrep.

Cyberoperasjoner skal være en del av planlegging og gjennomføring av FOHs fellesoperative innsats. I henhold til *FDs retningslinjer for informasjonssikkerhet og cyberoperasjoner* skal planlegging og ledelse av cyberoperasjoner «med mindre annet følger av gjeldende regelverk for gjennomføring av særlig sensitive etterretningsoperasjoner … følge ordinære operasjonsplanprosesser …Cyberoperasjoner skal underlegges politisk styring og kontroll på lik linje med øvrige operasjoner.» (ibid, s. 12). FOH opprettet i 2016 arbeidsgruppen Cyber Operations Working Group for å styrke den nasjonale evnen til å anvende cybermakt som en integrert komponent i fellesoperasjoner. Herunder inngår å øke cybersituasjonsforståelsen i Norges interesse- og ansvarsområder, utvikle konsepter og operative planverk hvor cybermakt understøtter operasjonelle målsettinger, og være rådgivende organ for FOHs ledelse innen

cyberoperasjoner. FOH gjennomfører jevnlige situasjonsoppdateringer med POD og NSM, hvor det militære bildet, politibildet og det sivile cyberbildet utveksles mellom de tre instansene for å styrke den nasjonale beredskapen. I en tid hvor skillet mellom fred, krise og konflikt er uklart og varslingstiden er minimal, er en god forståelse av normalsituasjonen i alle domener en forutsetning for forsvar og suverenitetshevdelse i alle domener – i hele konfliktspekteret.

Etterretningstjenesten – Offensive cyberoperasjoner og tidlig varsling

Etterretningstjenesten er Norges militære og sivile utenlands etterretningstjeneste og er organisatorisk underlagt Forsvarssjefen (FSJ). E-tjenesten har et nasjonalt ansvar, som ikke er begrenset til militære operasjoner. Sjef E-tjenesten er operativ sjef, sidestilt med sjef FOH, og støtter FOHs oppdragsløsning i fred, krise, krig og væpnet konflikt, med alle kapasiteter etter behov. E-tjenesten skal utføre tidlig varsling av mulige cybertrusler fra fremmede stater, organisasjoner eller individer, bidra i produksjon av nasjonalt cyberrisikobilde, være koordinerende myndighet innen cyberoperasjoner og gjennomføre offensive cyberoperasjoner (Forsvarsdepartementet, 2014, s. 18). E-tjenesten er avhengig av å kunne benytte nye virkemidler og metoder for å overvåke trafikk inn og ut av landet. Forslaget om å etablere et Digitalt Grenseforsvar (DGF) er et slikt virkemiddel (se Lysne et al., 2016). På denne bakgrunn har regjeringen besluttet å utrede og konkretisere hvordan en form for digitalt grenseforsvar kan etableres og lovreguleres, og særlig vektlegge hensynet til personvern og menneskerettigheter (Regjeringen, 2017b). I dag er E-tjenesten avhengig av å få denne informasjonen fra andre stater, og av informasjonen som eventuelt tilgjengeliggjøres via deres deltakelse i for eksempel FCKS.

Som Norges utenlands etterretningsorganisasjon er E-tjenesten en svært viktig bidragsyter til forsvar og suverenitet: For det første med etterretninger og tidlig varsling. For det andre som eneste aktør som er tillagt myndighet til å gjennomføre offensive cyberangrep mot andre stater som direkte eller indirekte utfordrer norsk suverenitet.

Cyberforsvaret – Forsvar av Forsvaret

Forsvarets avdelinger for IKT-drift, INI,[42] endret i 2012 navn til Cyberforsvaret (heretter Cyfor) og er i dag direkte underlagt Sjef FOHs kommando. Selv om navneendringen kom først i 2012, har informasjonssikkerhet og beskyttelse av Forsvarets IKT-systemer vært en del av organisasjonens oppgaver i mange år. Cyfor skal sikre, drifte og beskytte Forsvarets egne datasystemer og kommunikasjonsnettverk. Cyfor håndterer angrep mot Forsvaret gjennom overvåkning og defensive operasjoner i Forsvarets egen infrastruktur (Forsvarsstaben, 2014, s. 122). I tillegg leverer Cyfor infrastruktur og tjenester til deler av statsforvaltningen og andre aktører med sikkerhets- og beredskapsbehov.

Cyberforsvaret har et eget cybersikkerhetssenter[43] (Forsvarsdepartementet, 2012, s. 103) som samarbeider med NSM NorCERT og sentrale sivile aktører, som Telenor. Cyfor har mobile ressurser på beredskap som kan settes inn for å gjennomføre defensive cyberoperasjoner. Cyfor gjennomfører ikke defensive operasjoner utenfor Forsvarets infrastruktur, for eksempel i sivil infrastruktur som Forsvaret er avhengig av, eller offensive operasjoner. Cyfor har ikke ansvar for elektronisk krigføring eller beskyttelsestiltak mot fremmedstatlig elektromagnetisk påvirkning.

Cyfor skal i henhold til FDs cyberretningslinjer kunne støtte det sivile samfunnet (Forsvarsdepartementet, 2014, s. 12). Dette kan innebære bruk av Forsvarets materiell og utstyr, personell og kompetanse i særskilte situasjoner der sivile myndigheters ressurser ikke strekker til og Forsvarets kapabiliteter er relevante. Støtte til det sivile samfunnet er ikke en dimensjonerende oppgave for Cyfor, og i kriser vil det ikke være tilgjengelige ressurser til støtte for sivile aktører (Forsvarsdepartementet, 2017, s. 21-22). I nasjonale krisesituasjoner har Cyfor ressurskrevende arbeidsoppgaver hjemlet i *Beredskapssystem for forsvarssektoren* (BFF) og nasjonale operative planverk. BFF har rang foran bistandsinstruksen. Cyfors bistand

[42] INI: Forsvarets informasjonsinfrastruktur

[43] Tidligere kalt Avdeling for beskyttelse av kritisk infrastruktur (BKI). (Prop. 73 S (2011-2012), s. 103): «bidra til å beskytte Forsvarets infrastruktur gjennom støtte til analyse av sårbarheter, ondsinnet kode og angrep mot Forsvarets systemer. Avdelingen har deployerbare elementer og mulighet til å bistå med rådgivning og liaisonering ved håndtering av trusler og angrep mot norsk infrastruktur ute og hjemme»

til det sivile samfunnet vil derfor ikke være relevant i annet enn avgrensede episoder som treffer enkeltsektorer.[44]

Cyfors bidrag til statssikkerhet og til norsk suverenitet er å beskytte og forsvare Forsvarets nettverksbaserte kampkraft mot digital påvirkning fra fremmedstatlige aktører. Forsvarets utholdenhet og mottakssystem for alliert støtte er avhengig av sivile aktører og sivil infrastruktur, noe som ligger utenfor Cyfors ansvarsområde. Suverenitetshevdelse handler om å kunne bruke militærmakt, om nødvendig for å sikre og forsvare norske interesser. Cyberforsvaret besitter ikke midler for å utøve militærmakt, og kan derfor ikke *hevde* norsk suverenitet i cyberdomenet. Cyberforsvaret bidrar likevel til å *sikre* norske interesser, ved at Cyberforsvaret skal forsvare Forsvaret, som igjen skal hevde norsk suverenitet.

2.2.4 Nasjonalt samarbeid

Felles cyberkoordineringssenter

FCKS ble opprettet i 2017 og består av Norges etterretnings-, overvåkings- og sikkerhetstjenester (EOS-tjenestene) E-tjenesten, PST og NSM, samt KRIPOS. Senteret er en videreutviklingen av den tidligere cyberkoordineringsgruppen (CKG), ledes av NSM og ble opprettet for å øke informasjons- og erfaringsutveksling mellom tjenestene. Når et cyberangrep er alvorlig nok blir det løftet opp til FCKS som analyserer og vurderer om det er en sak for E-tjenesten, politiet, eller en enkeltstående sektor. Den enheten som ender opp med å lede håndteringen av hendelsen, støttes ved behov fra resten av FCKS og andre som hentes inn. FCKS er et koordinerende forum og har ikke beslutningsmyndighet.

[44] Poenget er understreket av FD: «Forsvaret kan innenfor cyber- og IKT-områdene yte bistand til sivile myndigheter basert på den kompetanse og kapasitet Forsvaret har for å ivareta de IKT-systemer forsvarssektoren selv benytter. Ressursene vil i situasjoner med fare for omfattende digitale angrep mot samfunnskritisk infrastruktur, primært måtte prioriteres til å ivareta sikring av Forsvarets egne IKT-systemer.» (Forsvarsdepartementet, 2017, s. 21-22)

Center for cyber and information security

Norge har ikke et militærindustrielt cyberkompleks som kan sammenlignes med Israel, men et mikrokompleks med 80 ansatte kalt Center for cyber and information security (CCIS). CCIS ble opprettet i 2014 og er et spleiselag mellom offentlig og privat sektor, delfinansiert av KMD, JD og Helse- og omsorgsdepartementet (HOD). CCIS er et samarbeid mellom industri, akademia, Forsvar og cybersikkerhetsmiljøer, og er lokalisert på Høyskolen i Gjøvik som en underavdeling av Norges tekniske og naturvitenskapelige universitet. CCIS ble opprettet for å øke Norges kapasitet innen langsiktige cybersikkerhetsutfordringer, utvikle cybersikkerhetskompetansen i nasjonale virksomheter og akademia, og støtte regjeringen i internasjonale samarbeidsfora, og senteret skal bidra til å styrke samfunnets evne til å beskyttelse, oppdage relevante trusler og håndtere aktuelle hendelser. Ved senteret er blant annet Cyberforsvaret, Politiet, NSM, NorSIS, Datatilsynet, Telenor, IBM og cybersikkerhetsselskapene Mnemonic og Watchcom tilstede. CCIS bidrar til grunnleggende IKT-sikkerhet i form av kompetanse og kunnskap – som kan bidra til å styrke motstandsdyktighet og nasjonal cybersikkerhet (CCIS, 2018).

2.3 Oppsummering

I det videre gis en sammenstilling av forskjeller og likheter mellom norsk og israelsk organisering av ansvar og roller for cybermakt innen forsvar, suverenitetshevdelse og myndighetsutøvelse – og avslutningsvis sivil-militært samarbeid.

2.3.1 Forsvar

Militært forsvar

Når det gjelder militært cyberforsvar, har Norge og Israel organisert seg relativt likt: Cyfor og C4iCDD har et ansvar for å beskytte og forsvare militær sektor. Både norsk og israelsk forsvarsevne er modernisert og digitalisert, og både Cyfor og C4iCDDs hovedoppdrag er forsvare land-, luft- og sjøstyrkenes kampkraft. Både Cyfor og C4iCDD skal kunne støtte

sivile myndigheter i krisesituasjoner, og begge har fremholdt at dette vil være problematisk. Men ikke alt er likt. Noen vesentlige forskjeller må fremheves.

Den første forskjellen er at C4iCDD angivelig skal forsvare *utvalgt sivil kritisk infrastruktur*. C4iCDD har da mulighet til å øve og trene sammen med eieren av den kritiske infrastrukturen i fredstid (eller mellom kriger), etablere sikringsplaner og avsette dedikerte ressurser til formålet. Det vil i prinsippet være på samme måte som Heimevernet øver og trener på fysisk objektsikring og etablerer objektsikringsplaner for *utvalgt* sivil kritisk infrastruktur. I krise og krig kan man med større sikkerhet enn i fredstid anslå hvem som står bak et fiendtlig cyberangrep, basert på den helhetlige sikkerhetspolitiske situasjonen og kunnskap om fiendens evne og kapasitet. C4ICDDs oppdrag om å beskytte *utvalgt* sivil kritisk infrastruktur i krisesituasjoner kan derfor være verdt en nærmere studie, for Norges del med henblikk på kritisk sivil infrastruktur som Forsvarets operasjoner avhenger av.

Den andre forskjellen er at C4iCDD har etablert egen etterretningskapasitet og offensive kapasiteter, og angivelig skal kunne gjennomføre aktivt forsvar og motangrep, i motsetning til Cyfors oppdrag som er mer passivt forsvar. Cyberforsvaret utfører ikke offensive mottiltak eller aktive tiltak[45] som har direkte effekter utenfor Forsvarets infrastruktur. Cyberforsvarets primæroppdrag er å forsvare Forsvaret. Om denne evnen uttalte Sjef cyberforsvaret, generalmajor Inge Kampenes, i et intervju med tittelen «Vi holder ikke lenge» følgende: «evnen til å oppdage alt er marginal. Og evnen til å analysere, er også marginal. Vi er marginale på hele spekteret av oppgaver – fra oppfylling av beredskapsbeholdning til treningsnivå til styrkestruktur til planverk.» *(Eide, 2017).* En tredje forskjell er at ISA gjennomfører cyberoperasjoner med defensive formål, i motsetning til PST i Norge. Det er også en likhet mellom Israel og Norge, at det i begge land er etterretningsorganisasjonene som har hovedansvaret for offensive cyberoperasjoner, selv om det i Israel tilsynelatende også er andre aktører som er gitt et mandat på området.

[45] Aktive tiltak er i dette tilfellet dedusert fra «AAP-6 NATO glossary of terms and definitions» (NATO Standardization Agency, 2014, s. '2-A-2') definisjon av «active defence» som brukes om tiltak rettet mot en motstander, for å forhindre, oppheve, eller redusere effekten av fiendtlige handlinger.

Beskyttelse av kritisk infrastruktur og samfunnskritiske funksjoner

Norge og Israel var blant verdens første til å opprette systemer for å ivareta beskyttelse av digital kritisk infrastruktur. CERT-IL tilhører NCSA under Statsministerens kontor. NSM NorCERT tilhører NSM under FD. Begge har et sektorovergripende ansvar, og begge organiseringer muliggjør bygging av en nasjonal situasjonsforståelse i cyberdomenet. Hovedforskjellen er at CERT-IL utfører aktiv beskyttelse av kritisk infrastruktur. I Norge har vi to koordinerende nivå før det kommer til aktiv utførelse – NSM NorCERT og de sektorvise responsmiljøene. Det laveste nivået, den enkelte virksomhet, må selv ivareta egenbeskyttelse – uavhengig av om angriperen er gutteroms-hacker eller en høykompetent statlig trusselaktør. Det er ikke gitt at Norges modell er dårligere i fredstid. Norge har senest i 2017 vist en relativt høy motstandsdyktighet mot verdensomspennende cyberangrep som «Wannacry», «Petya» og «NotPetya» (BBC, 2017; Minister for Law Enforcement and Cyber Security, 2018). Angrepene var ikke var målrettet mot Norge, men likevel gjennomført av de kompetente statlige aktørene Russland og Nord-Korea. I fredstid står kanskje Norge like sterkt mot denne type angrep – med ansvarsprinsippet og ansvarliggjøring av den enkelte sektor og eiere av kritisk infrastruktur – som Israels system som muligens bidrar til umyndiggjøring og ansvarsfraskrivelse på lavere nivå.

Israels fordel ligger i at beskyttelse av kritiske funksjoner og infrastruktur ikke er frivillig, og at tilnærmet all kritisk infrastruktur blir beskyttet. I Norge vil tilknytning til NSM NorCERTs VDI også etter ny sikkerhetslov være frivillig, selv om flere eiere av infrastruktur vil kunne pålegges tiltak for å beskytte seg. Cybermakt og cyberoperasjoner har blitt en arena for statlig og militær maktanvendelse, men hverken politiet, Cyberforsvaret eller E-tjenesten kan hver for seg forsvare sivil infrastruktur. Å ansvarliggjøre virksomheter om egen IKT-sikkerhet på laveste nivå kan sammenlignes med at man ansvarliggjør virksomheter til å beskytte seg selv med innbruddsalarmer og vektere mot tradisjonell kriminalitet. Det er med andre ord helt naturlig, også for Israel, som har utgitt en eget rammeverk for virksomheters egenbeskyttelse til dette formål. Forskjellen er at Israel skiller mellom IKT-sikkerhet og cybersikkerhet.

Det er et tankekors at man ved å overlate beskyttelse av samfunnets kritiske funksjoner mot fremmedstatlig militær cybermakt også overlater deler av norsk forsvarsevne til private og kommersielle aktører – i fred, krise og krig. Løsningen er ikke enkel, spesielt ikke i fredstid,

siden det ofte tar lang tid å attribuere (fastslå hvem som står bak) cyberangrep. Man kan heller ikke enkelt overlate beskyttelsen til politiet eller Forsvaret.

2.3.2 Suverenitetshevdelse

Suverenitetshevdelse er primært en oppgave for de væpnede styrkene både i Israel og Norge, og handler for begge om bruk av nødvendig militær makt for å sikre territoriell suverenitet og suverene rettigheter. Både i Norge og Israel er kapasiteter med hovedansvar for defensive og offensive cyberoperasjoner organisert som en del av de væpnede styrkene: I Norge ved Cyberforsvaret, med defensiv kapasitet, og Etterretningstjenesten, med offensiv kapasitet. I Israel er det C4iCDD, med hovedansvar for defensive cyberoperasjoner, og IDIs Unit 8200 med hovedansvar for offensive operasjoner. For Israels vedkommende kan Unit 8200 og C4iCDD, samt Mossad og ISA, gjennomføre offensive cyberoperasjoner og dermed hevde israelsk suverenitet og suverene rettigheter med militær (og paramilitær) makt. I Norge er det E-tjenesten som kan gjennomføre offensive cyberoperasjoner og hevde norsk suverenitet med militærmakt i cyberdomenet. Sjef E-tjenesten, Morten Haga Lunde, har sagt følgende om formålet med og behovet for DGF:

> «De mest avanserte truslene i det digitale rom kan i dag ikke avdekkes med tilgjengelige metoder. Dette gjelder i særdeleshet statlig spionasje og forberedelser til cyberangrep, samt grenseoverskridende terrorplanlegging. I dag er vi prisgitt tips fra partnere, som har DGF-lignende ordninger, men som av naturlige grunner ikke prioriterer norske interesser først.» (Etterretningstjenesten, 2017a)

Cyberforsvaret kan forsvare Norges suverene rettigheter i Forsvarets del av cyberdomenet, men har ingen maktmidler og kan derfor ikke hevde norsk suverenitet med militærmakt. Resten av Forsvaret kan, dersom en krenkelse av norsk suverenitet i cyberdomenet anses som alvorlig nok, bruke andre former for militærmakt enn cybermakt for å hevde norsk suverenitet. Det siste gjelder også for Israel.

2.3.3 Myndighetsutøvelse

Sammenligningen viser at Norge ikke står tilbake for Israel når det gjelder systematisk og statlig regulering av myndighetsutøvelse i cyberdomenet selv om organiseringen er ulik.

I Israel ligger ansvaret for myndighetsutøvelse på Cyberdirektoratet med INCB og NCSA som utøvende organer. I Norge er hovedansvaret for myndighetsutøvelse for forebyggende cybersikkerhet tillagt NSM som er underlagt FD. I tillegg har følgende norske departementer og direktorater oppgaver og ansvar som i Israel delvis er tillagt Cyberdirektoratet: JD med deler av DSB, SD med Nkom, KMD med Datatilsynet og Difi samt Kunnskapsdepartementet (KUD).

Når det kommer til politiets myndighetsutøvelse i Israel og Norge, er det flere likheter. Organiseringen er i prinsippet lik. Både i Israel og Norge har politiet svært begrenset evne til å forebygge og etterforske fremmedstatlige cyberangrep, og oppgavene er begrenset til reaktiv myndighetsutøvelse. Begge har nylig etablert egne cybercrime-sentre. Hovedforskjellene finner vi hos PST og ISA. PST er underlagt JD, mens ISA er direkte underlagt PMO. ISA har lang erfaring med cyberoperasjoner, både defensive (med bakgrunn i tidligere hovedansvar for NISA og beskyttelse av kritisk infrastruktur) og offensivt, eller proaktivt, i kampen mot terror. PST på sin side har begrensede ressurser for utføre sitt oppdrag og politiet fremholder følgende i sin egen datakrimstrategi:

> «Digital etterretning utført av fremmede stater vil som regel være vanskelig å straffeforfølge. … Det viktigste virkemiddelet vil derfor være å informere aktørene som er utsatt for ondsinnet etterretning, om hva de står overfor, og hvordan de kan redusere sin egen sårbarhet. Et annet virkemiddel kan være politiske reaksjoner, men dette vil oftest ha liten effekt.» (Politidirektoratet, 2015, s. 81-82)

ISA kan i tillegg gjennomføre operasjoner og utøve myndighet utenfor israelsk territorium. Organiseringen og ansvaret mellom Etterretningstjenesten og PST er i Norge klart adskilt: utenriks og innenriks. Selv om utfordringene de står overfor er grenseoverskridende, kan de ikke krysse hverandres grenser. Utfordringen søkes løst gjennom koordinering i FCKS. I Israel er også *hovedansvaret* mellom sikkerhets- og etterretningstjenestene klart definert, men de kan krysse hverandres grenser så lenge det er koordinert. I Norge søker å ha klart definerte grenser.

Ytterligere en forskjell er at IDFs C4iCDD har begrenset myndighetsutøvelse gjennom oppdraget om beskyttelse av utvalgt kritisk infrastruktur i krisesituasjoner. Cyfor på sin side *kan* støtte sivile aktører etter anmodning ved kriser, men har begrensede ressurser, og oppdraget er ikke dimensjonerende.

2.3.4 Sivil-militært samarbeid

Den viktigste forskjellen mellom norsk og israelsk sivilmilitært samarbeid finner vi i Israels militærindustrielle cyberkompleks, hvor myndigheter, forsvar, industri og akademia deltar. Kompleksets hovedformål er å styrke cybersikkerheten, og dermed statssikkerheten, for Israel og det bidrar samtidig til å styrke israelsk økonomi. I Norge har vi et mikro-kompleks på Gjøvik og en rekke andre offentlig og private koordineringsgrupper, men ingenting som kan måle seg i størrelse og betydning.

2.4 Delkonklusjon

Som vist i sammenstillingen er det svært mange likheter i organiseringen av cybermakt i Norge og Israel. Både Norge og Israel besitter i sum stort sett de samme organisatoriske enhetene som bidrar til cybermakt. Hverken Norge eller Israel har DGF-lignende løsninger[46], og begge står overfor det samme demokratiske dilemma hvor de mangler en modernisert lovgivning som ivaretar både personvernet og statssikkerheten.

De viktigste forskjellene i organiseringen av cybermakt er:

- Israels sentralstyrte Cyberdirektorat kontra ansvarsprinsippet i Norge.
- Det militærindustrielle cyberkomplekset som det ikke finnes tilsvarende av i Norge.
- Ansvaret for offensive cyberoperasjoner er distribuert på flere enheter i Israel.

De organisatoriske forskjellene kan ikke alene forklare hvorfor Israel er en cyberstormakt, mens Norge befinner seg i en situasjon med avmakt i cyberdomenet. Vi skal derfor også studere hvordan de to lands ulike prinsipper for cybermakt kan bidra til å forklare forskjellene.

[46] Litteraturen som denne studien er bygd på har ikke påvist at Israel har implementert løsninger for masseovervåkning. Det er imidlertid ikke alt som oppgis i åpne kilder.

3 Komparativ analyse del II – Prinsipper for cybermakt

Både i Norge og Israel er cybermakt en del av det politiske og militære maktinstrumentet, men hverken Norge eller Israel har utformet konkrete prinsipper for utnyttelse av cybermakt. Denne delen vil ta for seg overordnet politikk, offentlige uttalelser og sentrale strategidokumenter i et forsøk på å avdekke hvilke dominerende prinsipper som ligger til grunn for anvendelse av cybermakt i de to landene.

3.1 Israelske prinsipper for cybermakt

For Israel er militære prinsipper fundamentert i strategiske tenkning. General Yigael Yadin, sjef for generalstaben under den første arabisk-israelske krig i 1948 – 1949, uttrykte seg slik:

> «every principle which the enemy is likely to apply must serve as a target for the ingenuity of those who plan the operations of our forces. … Against the principle of **maintenance-of-aim** – tactical diversionary attacks and strategical, psychological and political offensives. Against the principle of **economy of force** – attacks against lines of communicatons and stores in the rear, thereby pinning down the enemy's forces and dispercing them. … Against the principle of **offensive spirit** – offensive spirit.» (mine uthevinger) (Yadin, 1991 [1949], s. 386)

Sitatet over er et utvalg av tre sentrale prinsipper med opprinnelse i J. F. C. Fuller[47] som er tydelige i Israels utøvelse av cybermakt.

[47] Fullers prinsipper har hatt ulike uttrykk men er ofte gjengitt slik: 1) The Principle of the Objective, 2) The Principle of the Offensive, 3) The Principle of Mass, 4) The Principle of Economy of Force, 5) The Principle of Maneuver, 6) The Principle of Unity of Command, 7) The Principle of Security, 8) The Principle of Surprise, 9) The Principle of Simplicity (se Fuller, 1926; Forsvarsstaben, 2014, s. 83)

Jeg vil på dette grunnlag argumentere for at israelsk cybermakt er basert på grunnprinsipper for militær krigføring[48]:

- Felles mål og enhetlig ledelse
- Strategisk styrkeøkonomisering
- Offensiv opptreden

Dette kapittelet vil ta for seg hovedtrekkene ved israelsk cybermakt og drøfte Norges posisjon i lys av disse særtrekkene.

3.1.1 Felles mål og enhetlig ledelse

Israels taktiske, operasjonelle og strategiske tenkning har tradisjonelt vært preget av hemmelighold og skjult for omverden, men de siste årene har det skjedd en endring med mer åpenhet fra strategisk og politisk nivå. Israels første offentlige militære doktrine ble utgitt i 2015, og Israels statsminister Benjamin Netanyahu har uttrykt en tydelig ambisjon om å bli en av verdens ledende cybermakter. Israel ser i dag på seg selv som en av «de fem store» sammen med USA, Storbritannia, Russland og Kina, egentlig kun overgått av USA (Netanyahu, 2016).[49]

David Ben-Gurion, Israels første statsminister og samtidig forsvarsminister, formulerte en strategisk visjon om et uavhengig Israel, og fastsatte prinsipper og modus operandi ansett som kritiske for både opprettelsen av og eksistensen til staten Israel (Yanai, 1989, s. 151, 162). Ben-Gurions visjoner har i ettertiden vært kjent som Israels offisielle sikkerhetsdoktrine, med fred som det ultimate målet. Veien mot fred var aksept for Israels eksistens blant araberstatene. Doktrinen var basert to prinsipper: en folkehær, og det såkalte «sikkerhetstriangelet». Sikkerhetstriangelet innebar de tre elementene avskrekking, tidligvarsling og, i tilfelle krig, en rask og avgjørende seier (Baram, 2017, s. 2-3). Målsettingen om å sikre fred og den israelske statens eksistens, til tross for manglende

[48] Det er verdt å bemerke at militære prinsipper ikke kan anses som allmenngyldige og universelle, men at de likevel påvirker militær tenking i både Norge og Israel (Høiback & Ydstebø, 2012, s. 64-67)

[49] Slike utsagn kan tjene mange formål, men reflekterer uansett svært høye ambisjoner.

anerkjennelse av araberstatene, kunne oppnås gjennom å overvinne motstanderne militært eller gjennom avskrekking og opprettholdelse av status-quo. Som en småstat omgitt av naboer som ikke anerkjente Israels eksistens, insisterte Ben Gurion etter Suezkrisen i 1956 også på at forsvarsevnen – som senere inngikk i konseptet kjent som «the iron wall», måtte baseres på *kvalitet og teknologisk overlegenhet* for å jevne ut ubalansen mot de kvantitativt overlegne araberstatene (Shlaim, 2014, s. 199-200).

Israel har en tradisjon for å bygge høyteknologisk forsvarsevne, noe det har både lykkes og feilet med. Yom-Kippur krigen i 1973 kom som en total overraskelse på Israel, som var av den oppfatning at det med bakgrunn i sin teknologiske overlegenhet også hadde informasjonsoverlegenhet. De tok feil. Israels suksess i krigen tilskrives i hovedsak tydelig ledelse, kamperfaring og vilje – ikke teknologisk overlegenhet (Paret, Craig, & Gilbert, 1986, s. 790-792).

Israel mistet ikke sin tro på teknologiens potensial etter Yom-Kippur krigen. Ben-Israel og Tabansky (2011, s. 25) beskriver hvordan Israel fra 2000 til 2005 klarer å kontre og vinne over palestinske selvmordsbombere ved hjelp av høyteknologisk krigføring. Suksessen hevdes å være et direkte resultat av Israels RMA (Revolution of Military Affairs), hvor nøkkelfaktorene er integreringen av informasjonsteknologi for å oppnå overlegen presisjonsstyrt ildkraft, manøver og informasjonskrigføring. Men Israel møter fra midten av 2000-tallet en ny type trussel som utfordrer troen på informasjonsteknologiens betydning for krigføringen; en trussel som ikke direkte kan møtes med overlegen høyteknologisk ildkraft. Den nye trusselen har en hybrid karakter[50] og påfører IDF nederlag (eller i det minste mangel på suksess) i krigen mot Hizbollah i 2006 (Hoffman, 2007, s. 17-42). Under krigen mellom Israel og Hizbollah i Libanon trekkes overdreven digitalisering av det israelske forsvaret frem som en av grunnene til israelsk manglende seier. Dette, og svakheter i etterretning,[51] påførte

[50] Hybrid krigføring, hvor en utnytter både geriljataktikk og konvensjonelle midler, har vi sett eksempler på fra både Hizbollah i 2006 (Hoffman, 2007), og fra Russlands annektering av Krim «med alle statens midler» i 2014.

[51] Israel befant seg etter mange år med intifadaoperasjoner, hvor de hadde informasjonsoverlegenhet gjennom god etterretning og utnyttelse av høyteknologiske sensornettverk, i en situasjon hvor de ikke hadde tidsriktig og brukbar etterretning (se Glenn, 2012, s. xii).

Israel en informasjonsunderlegenhet i konflikten. IDFs effektbaserte doktrine ble beskrevet som ubegripelig og vanskelig å omsette til kamphandling.

Opprørsbevegelser og terrornettverk har tilpasset seg vestlig utnyttelse av teknologi, ved blant annet å skjule seg blant befolkningen og unnlate å bruke teknologi som kan gjøre dem sårbare for motangrep. Den vestlige formen for krigføring med stor vekt på informasjonsoverlegenhet, muliggjort gjennom nettverkstenkning og utnyttelse av informasjonsteknologi, hadde gjort Israel mer kapabel, men også tilført nye sårbarheter. Israel måtte tenke nytt i lys av erfaringer fra situasjoner der slike sårbarheter ble utnyttet av Hizbollah og Israels motstandere i den såkalte elektroniske intifadaen, herunder hvordan den palestinske motstandsbevegelsen utnyttet digitale påvirkningsoperasjoner for å så internasjonal tvil om den israelske krigføringen (se Yin, 2009).

Ben-Israel forteller i et intervju at han i 2010 anbefalte Netanyahu å gjøre Israel til et globalt cybersikkerhetssentrum. I følge Ben-Israel nølte Netanyahu aldri, og en milliard shekel[52] ble avsatt til formålet (Horovitz, 2017).

Hvorfor forfølger Israel målsettingen om å være en av verdens største cybermakter? Studerer vi dagens sikkerhetsdoktrine, ser vi at overlevelse fortsatt er en sentral målsetting, og at Israels anvendelse av cybermakt primært er et middel for å sikre statens overlevelse. Israels målsettinger, og utviklingen av cybermakt, var innledningsvis drevet av militær tenkning og militære målsettinger, men forankret i statens høyeste politiske målsettinger. Den politiske forankringen kom etter hvert – og de positive effektene cybermakten har for israelsk økonomi og diplomati kan i dette perspektivet sies å være den militære cybermaktens *indirekte* effekter.

3.1.2 Strategisk styrkeøkonomisering

I Israel er forsvar og cybersikkerhet samfunnsnyttig verdiskapning, hvor investering i forsvar ikke tapper økonomien, men styrker den. Økonomisering og lønnsomhet bør sees i et verdiperspektiv opp mot nasjonens interesser. Om dette skriver J. F. C. Fuller: «In its ultimate

[52] Tilsvarer ca 2,3 milliarder i 2018 NOK.

form the economic object in war is the national object, namely, survival with profit» (Fuller, 1926, s. 73). Det ultimate målet i strategisk styrkeøkonomisering av cybermakt er at nasjonen profiterer, mentalt, moralsk og fysisk, på investering i nasjonal sikkerhet og statens overlevelse. For å forstå denne dynamikken er det nødvendig å analysere det militærindustrielle cyberkomplekset.

Israels suksess kan i hovedsak tilskrives forskning og utvikling, ikke kontroll og styring (Netanyahu, 2017). Israels cyberkompleks tar sikte på å samle alle aktører med sammenfallende interesser på ett sted: Spark-senteret i byen Beer Sheba i Negev-ørkenen. Spark er på størrelse med en liten by og huser både Israels nasjonale cyberbyrå (INCB), Israels nasjonale CERT, over 10000 IDF-veteraner (fra Unit 8200 og C4iCDD), små og store kommersielle nasjonale og multinasjonale cybersikkerhetsselskaper, utdanningsinstitusjoner og forsknings- og utviklingsmiljøer (Cyberspark, 2018). I dette økosystemet bidrar myndighetene med incentiver, IDF med ekspertise, akademia med ideer, investorer med finansiering og industrien med teknologiske løsninger, som igjen kan utnyttes til forsvaret av Israel. Spark er uten tvil et konglomerat av aktører med motstridende målsettinger, men en samling av alle disse aktørene bidrar også til at IDF, investorer og kommersielle aktører finner felles interesser og målsettinger.

Siden 1979 har IDF hatt et program kalt «Talpiot», som går ut på å selektere, utdanne og forberede de beste soldatene til å gå inn i lederstillinger innen teknologi i IDF og forsvarsindustrien (Paikowsky & Ben Israel, 2009, s. 1465). Rekruttene blir gitt tre års lederutdanning og høyere teknologisk utdanning etterfulgt av seks års militær erfaring innen taktikk, teknologi og lederskap. Etter endt tjeneste ender mange av dem opp som cybersikkerhetsentreprenører i cyberkomplekset. Myndighetene har et eget program som sponser denne type entreprenørskap. Unit 8200 og C4iCDD tar inn soldater til tre års verneplikt og spesialiserer dem i cyberoperasjoner. Ambisjonen er å styrkeprodusere 2000 – 3000 eksperter årlig til cyberkomplekset (Cyberspark, 2018).

IDF er til stede der hvor verdens fremste cybersikkerhetsmiljøer er samlet, det er til stede der hvor teknologi og ideer skapes, det kan fremme egne behov for å stimulere til utvikling, og det kan hente metoder og verktøy til bruk i både defensive og offensive operasjoner. Dette gir staten mulighet til å høste lavthengende frukter i form av nyskapende ideer, den nyeste

teknologien, de smarteste hodene og banebrytende taktikker. De internasjonale kommersielle aktørene i cyberkomplekset kan velge å holde teknologiske nyvinninger for seg selv, de kan velge å holde nyoppdagede sårbarheter for seg selv, de kan velge å selge internasjonalt, eller de kan velge å selge kun til Israel.

3.1.3 Offensiv opptreden

Israel har gjort seg bemerket som en stat som har evne til å gjennomføre avanserte offensive cyberoperasjoner. «There are five top players. Offensively and defensively, they're the same. Not in order: Israel, the US, Russia, Britain, China» (Ben-Israel, sitert i Horovitz, 2017, s. 6). Spesielt hyppig nevnes operasjon Olympic Games: Stuxnet-angrepet på Irans atomprogram som ble oppdaget i 2010 (Rid, 2013, s. 96, 99-100), og operasjon Orchard; hvor det Israel-attribuerte cyberangrepet tilrettela for bombing av det påbegynte atomprogrammet i Syria i 2007 (Ward, 2007). Den digitale utviklingen går raskt, og det er i det digitale perspektivet lenge siden disse angrepene fant sted.

Offensiv evne og opptreden henger også tett sammen med avskrekking. Diskusjonen om cyberavskrekking har pågått i flere år uten enighet i forskermiljøene (se for eksempel Fischerkeller & Harknett, 2017; Jervis, 2016; Muller, 2017). På generelt grunnlag bunner denne uenigheten ut i at cybermaktens potensial fortsatt er uviss og preget av en rekke antakelser om den faktiske trusselen. Teorier om avskrekking vokste frem med atomvåpenkappløpet under den kalde krigen. En diskusjon om cybermakt og avskrekking kan ikke holdes avskjermet til cyberdomenet. Avskrekking skjer i den kognitive dimensjonen, og diskusjonen om avskrekking i cyberdomenet *alene* er derfor irrelevant. Avskrekking ved hjelp av cybermakt som har effekter utover cyberdomenet gjør debatten mer relevant. Digitale påvirkningsoperasjoner og subversjon brukes for å skape sosial uro, nøre opp under motsetninger, og påvirke demokratiske prosesser (eksempelvis valget i USA[53] og den elektroniske intifada for å undergrave oppslutningen om Israel internasjonalt).

[53] Se *JAR-16-20296: Grizzly Steppe – Russian Malicious Cyber Activity* (FBI & Department of Homeland Security, 2016).

Israelsk cybermakt er preget av en kost-nytte tankegang. Israel har veid argumentet om atomvåpen i hendene på Iran og Syria som tyngre enn eventuelle konsekvenser av at cyberangrepene feilet (eller ble attribuert til Israel). Det er også mulig at Israel har vurdert det slik at en avsløring ville styrke avskrekkingen, uten å bidra til økt ustabilitet.

Israels offensive opptreden og bruk av offensive cyberstridsmidler kan bidra til å akkumulere israelsk avskrekking, men er ikke avskrekkende i seg selv. Israels økte satsning på defensiv cybermakt gjennom det militærindustrielle cyberkomplekset opprettholder deres evne til å gjennomføre offensive handlinger. Israels defensive styrking kan i tillegg være avskrekkende overfor regionale motstanderes vilje til å bruke cybermakt mot Israel, ved at kostnaden av å utvikle cybervåpen blir høyere enn verdien av potensielle cyberangrep. Selv om den offensive opptredenen kan ha akkumulert ekstra kapital på Israels konto for avskrekking, kan den samtidig ha forverret det sikkerhetspolitiske klimaet mellom Israel og araberstatene.

3.1.4 Oppsummering

IDFs anvendelse av cybermakt har vært offensivt rettet – mot eksistensielle trusler, og har i tråd med israelsk strategi fokusert målrettet på skjult ødeleggeleggelse av fiendtlige initiativ og akkumulert avskrekking. IDFs ambisjoner og målsettinger innen cybermakt var opprinnelig initiert nedenfra og opp, men likevel forenelige med Israels høyeste politiske målsetting – overlevelse. Den militære ambisjonen og statens grunnleggende politiske målsettinger har beredet grunnen for enhetlig ledelse, og det er dette som utgjør hovedstyrken i Israels cybermakt. Møtet mellom militær ambisjon og politiske mål bidro til å skape det militærindustrielle cyberkomplekset. Det utgjør en strategisk styrkeøkonomisering som forsterker israelsk økonomi og forsvarsevne – to grunnleggende forutsetninger for statens overlevelse.

3.2 Norske prinsipper for cybermakt

Norske militære prinsipper er ikke så synlig på militærstrategisk nivå som i Israel, men de har en sentral plass i Forsvarets fellesoperative doktrine (FFOD) og i planlegging og

gjennomføring av operasjoner på fellesoperativt og taktisk nivå. Det mangler ikke strategidokumenter[54] i Norge, men det er ikke så enkelt å identifisere prinsipper som er gjennomgående fra politisk nivå til militær anvendelse av cybermakt.

Den videre drøftingen tar utgangspunkt i de israelske prinsippene for cybermakt, og sammenligner funn fra norske strategidokumenter med disse israelske prinsippene.

3.2.1 Felles mål og enhetlig ledelse?

Forsvarets gjeldende strategiske konsept, *Evne til innsats*, presenterer fem overordnede sikkerhetspolitiske mål:[55]

> «Å forebygge krig og fremveksten av ulike trusler mot norsk og kollektiv sikkerhet.
>
> Å bidra til fred, stabilitet og videre utvikling av en FN-ledet internasjonal rettsorden.
>
> Å ivareta norsk suverenitet, norske rettigheter, interesser og verdier og beskytte norsk handlefrihet overfor politisk, militært og annet press.
>
> Sammen med våre allierte forsvare Norge og NATO mot anslag og angrep.
>
> Å sikre samfunnet mot anslag og angrep fra statlige og ikke-statlige aktører» (Forsvarsdepartementet, 2009, s. 8)

Om vi holder fast på den israelske definisjonen om at cybersikkerhet for en stat til syvende og sist handler om sikkerhetspolitikk: Understøtter norske mål og ambisjoner innen cybersikkerhet og cybermakt de overordnede sikkerhetspolitiske målene?

---

[54] Dette avsnittet tar kun for seg de viktigste strategidokumentene for cybersikkerhet. I tillegg finnes det en rekke tverrsektorielle og sektorvise strategidokumenter. Se for eksempel: *Difis tverrgående digitaliseringsstrategi (2018), Overordnet nasjonal strategi for bekjempelse av datakriminalitet (Datakrimstrategien), Nasjonal strategi for IKT forskning og utvikling (2013-2022)* og *Forsvarsdepartementets strategi for informasjonssikkerhet i forsvarssektoren (2017).*

[55] Det sikkerhetspolitiske bildet er riktignok endret siden 2009 og deler av konseptet kan argumenteres utdatert, men det er fortsatt det gjeldende, og de sikkerhetspolitiske målsettingene er ikke vesentlig endret.

Det er i hovedsak FD og JD som har ansvaret for å forme nasjonale mål for cybersikkerhet og cybermakt, men fordi strategi og forsvarbarhet i cyberdomenet ikke kan frikobles fra teknologiutviklingen, så er også KMD, som har ansvaret for Norges IKT-politikk, en viktig aktør.

I Norge finnes det ingen offentlig, overordnet politisk ambisjon om cybermakt. Norge har ingen strategi for cybersikkerhet, men en *Nasjonal strategi for informasjonssikkerhet.*[56] Strategien er fortsatt gjeldende og trekker opp tre relevante målsettinger: «1. Styrket samordning og felles situasjonsforståelse 2. «Robust og sikker IKT-infrastruktur i hele samfunnet 3. Sterk evne til å håndtere uønskede IKT-hendelser» (Departementene, 2012, s. 17). Strategiens tittel og målsettinger indikerer at strategiens fokus er informasjons- og IKT-sikkerhet, ikke cybersikkerhet, nemlig å sikre nasjonale interesser. I praksis tar strategien likevel enkelte grep som strekker seg utover informasjons- og IKT-sikkerhet og adresserer cybersikkerhet. For eksempel pålegger den hver enkelt sektor og *samfunnskritiske funksjoner* å etablere et responsmiljø for å koordinere og håndtere uønskede hendelser. Det kommer ikke direkte frem av strategien hvordan den skal understøtte Norges overordnede politiske målsettinger, men strategien kan likevel ha bidratt til å gjøre samfunnet mer robust og motstandsdyktig, spesielt med videreutviklingen av NSM NorCERT og VDI. Strategien har hovedfokus på samfunnssikkerhet og treffer således den overordnede sikkerhetspolitiske målsettingen: «Å sikre samfunnet mot anslag og angrep fra statlige og ikke-statlige aktører» (Forsvarsdepartementet, 2009, s. 8). Det kommer imidlertid ikke frem hvordan statssikkerheten for øvrig skal ivaretas, eller hvordan alle sektorer skal bli i stand til å utøve selvforsvar mot fremmedstatlig digital etterretning og sabotasje.

I tillegg til denne nasjonale strategien utga UD i 2017 en *Internasjonal cyberstrategi for Norge*. Strategien fokuserer på bevaring av den internasjonale rettsorden, demokratiske rettigheter, ytringsfrihet og norske økonomiske interesser og trekker opp Norges strategiske

[56] *Nasjonal strategi for informasjonssikkerhet* kom første gang ut i 2003 (Regjeringen Bondevik II, 2003). Den gjeldende engelske versjonen av har fått navnet *Cyber Security Strategy for Norway*. Det ble i Meld St. 10 (2016-2017) varslet at FD og JD skal utarbeide en ny nasjonal strategi for IKT-sikkerhet, som skal angi regjeringens mål og strategiske prioriteringer innenfor IKT-sikkerhetsområdet.

prioriteringer.[57] Den internasjonale cyberstrategien vektlegger småstatsrealismen og den internasjonale rettsorden for å sikre egen overlevelse, men er også en tydeliggjøring av norsk ideal- eller moralpolitikk og forsiktig maktbruk (se Berg, 2018). Selv om strategien ikke eksplisitt uttrykker noen ambisjon om cybermakt kan det faktum at strategien kobles direkte til noen av Norges overordnede politiske målsettinger tolkes som et forsøk på å utøve myk makt gjennom cyberdomenet på den internasjonale arena. I tillegg kan alliansepolitikkens rolle i norsk sikkerhetspolitikk spores til strategiens mål om å: «utvikle god beskyttelse mot cybertrusler nasjonalt, herunder gjennom bredt sivilt- militært og offentlig-privat samarbeid [og] sammen med likesinnede land videreutvikle evnen til forsvar mot digitale angrep» (Utenriksdepartementet, 2017, s. 9).

FDs cyberretningslinjer fastslår: «Formålet med cyberretningslinjene er å bidra til å sikre nødvendig handlefrihet i cyberdomenet, og å unngå eller redusere konsekvensene av alvorlige cyberangrep rettet mot egne systemer.» (Forsvarsdepartementet, 2014, s. 4). Retningslinjene gjelder for forsvarssektoren – herunder Etterretningstjenesten, NSM, FOH og Cyberforsvaret. Målsettingen om handlefrihet i cyberdomenet må sees som en direkte ambisjon for oppfyllelse av den sikkerhetspolitiske målsettingen: «Å ivareta norsk suverenitet, norske rettigheter, interesser og verdier og beskytte norsk handlefrihet overfor politisk, militært og annet press.» (Forsvarsdepartementet, 2009, s. 8). Men som vi har sett i analysen av norsk organisering har Forsvarets aktører i cyberdomenet begrensede forutsetninger for å oppfylle Norges overordnede sikkerhetspolitiske mål. FD har heller ikke utdypet hva som ligger i «handlefrihet i cyberdomenet». Skuler vi i tillegg til Forsvarets investeringsplan er det tydelig at det ikke er samsvar mellom overordnede målsettinger og utvikling av *forsvarbarhet* i cyberdomenet, det vil si utviklingen av evnen til å beskytte Forsvaret – her gjennom investeringer i cybersikkerhet. Fokuset ligger på interneffektivisering, selv om robusthet og interoperabilitet også har funnet plass. Først i 2022 skal evne til cyberforsvar styrkes (Regjeringen, 2018).

[57] Blant disse er cybersikkerhet, innovasjon og økonomi, utvikling og markedstilgang, bekjempe kriminalitet gjennom internasjonalt samarbeid, cyberdomenets plass i sikkerhetspolitikken, global forvaltning av internett, utnyttelse av cyberdomenet for å fremme vekst, velstand og sikkerhet for alle, og frihet på nett (Utenriksdepartementet, 2017, s. 5-12).

For Norge, som befinner seg i et fredelig hjørne av verden og ikke frykter krig, har de politiske målsettingene et mer fredelig uttrykk enn i Israel. Det er ikke målsettingen om overlevelse som står høyest på den norske agendaen, men økonomisk vekst og fordeling. Selv om prinsippene for norsk cybermakt ikke er like tydelig uttrykt som i Israel, finnes det likevel spor i de forskjellige strategidokumentene som knytter tiltak til overordnede sikkerhetspolitiske målsettinger.

I militære operasjoner er enhetlig kommando og tydelige mål viktige prinsipper. De skal blant annet bidra til et hurtigere operasjonstempo enn fienden og øke beslutningsdyktigheten. Antallet strategidokumenter, delvis mangel på felles målsettinger og ansvarsprinsippet bidrar ikke nødvendigvis til å tilskynde enhetlig ledelse og felles mål. Israel har konkludert med at cybersikkerhet og cybermakt handler om strategi og politikk, og dessuten om utvikling, utdanning og teknologi, og har derfor samlet dette i et sentralstyrt direktorat.

3.2.2 Strategisk styrkeøkonomisering?

Selv om Norge ikke har noe som er sammenlignbart med Israels militærindustrielle cyberkompleks, finnes et annet kompleks, nemlig totalforsvaret. De siste år har vi sett ambisjoner om å fornye innholdet i totalforsvarskonseptet. Det opprinnelige totalforsvarskonseptet ble utviklet etter andre verdenskrig og skulle sikre støtte til Forsvaret i tilfelle krig eller alvorlige sikkerhetsutfordringer: «Grunnprinsippet i det tradisjonelle totalforsvarskonseptet var at samfunnets samlede ressurser om nødvendig skal kunne mobiliseres for forsvaret av landet» (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2015). Det fornyede totalforsvarskonseptet skal sikre gjensidig støtte mellom Forsvaret og resten av samfunnet i både fred, krise, væpnet konflikt og krig. Dette er en form for strategisk styrkeøkonomisering hvor småstaten bruker tilgjengelige virkemidler på best mulig måte. Den nasjonale økonomiske gevinsten er dog ikke en tydelig effekt av samarbeidet slik som i Israel. Cybersikkerhet og cyberforsvar har også en plass i det nye totalforsvarskonseptet, og prinsippet om gjensidig støtte og samarbeid i fred, krise og krig gjelder også i cyberdomenet. Analysen av norsk organisering har imidlertid vist at ved kriser i fredstid har forsvarssektoren lite å bidra med til sivile aktører, utover NSMs koordinerende rolle.

I norsk politikk, som handler mindre om overlevelse og mer om økonomi, er det ikke mangel på ambisjoner om bedre utnyttelse av samfunnets ressurser. «Totalforsvarskonseptet gir vide rammer for det sivilt-militære samarbeidet. … Det handler om en best mulig utnyttelse av samfunnets samlede beredskapsressurser, og er derfor god samfunnsøkonomi … Best mulig utnyttelse av fellesskapets ressurser er en viktig del av forsvarssektorens samfunnsansvar.» (Forsvarsdepartementet, 2017, s. 16-22). De norske initiativene er med andre ord av mer begrenset art og for å støtte samfunnssikkerhet, ikke statssikkerhet (forsvar og suverenitet).[58]

I Norge har vi et lignende system som Israels cyberkompleks, dog med en noe annen funksjon og basert på multistakeholder-initiativer[59]. Deler av cyberdomenet, spesielt internett, kan sees på som både internasjonalt og anarkisk og passer således inn i teorien. Både Israels cyberkompleks og multistakeholder-initiativet tar utgangspunkt i å investere i forskning, utvikling og teknologi som gagner statlige og kommersielle fellesinteresser. I Norge kan vi legge to systemer inn i multistakeholder initiativer: NSMs samarbeid med alle sektorer og private aktører, og mikro-komplekset CCIS på Gjøvik. Som analysen av organisering viste, bidrar likevel ikke NSMs samarbeid med sivile aktører til styrkeøkonomisering, men heller en rivalisering mellom privat og offentlig sektor. CCIS er for smått til å kunne gi sammenlignende effekter.

3.2.3 Offensiv opptreden?

I Norge som i Israel er det liten åpenhet om kapasitet og evne til å gjennomføre offensive cyberoperasjoner. Som beskrevet i analysen om norsk organisering, er det E-tjenesten som har

[58] Det samme kommer til uttrykk i stortingsmeldingen *IKT-sikkerhet – et felles ansvar* (se Justis- og beredskapsdepartementet, 2017).

[59] Slike initiativer er fundamentert på neo-liberalistisk teori, med utgangspunkt i internasjonale organisasjoners evne til å oppnå kollektive målsettinger i anarkiske miljø (Sterling-Folker, 2010, s. 129). Se for eksempel DeNardis & Raymond (2013) artikkel *Thinking Clearly About Multistakeholder Internet Governance* for en utfyllende beskrivelse av teorien.

evne og kapasitet til å gjennomføre offensive cyberoperasjoner. Norge har ikke tradisjon for offensiv opptreden i fredstid, slik som Israel har.[60]

FFI skriver om offensiv cybermakt: «Avanserte cyberoperasjoner med et høyt ambisjonsnivå er krevende og forutsetter innsats av meget store ressurser over tid. Cybermakt endrer derfor ikke maktforholdene i verden grunnleggende ved å oppheve forskjellen på stormakter og småstater.» (Eggen, 2013, s. 2). FFIs første del av utsagnet er relatert til offensive cyberoperasjoner og har bred støtte i akademiske miljøer (se for eksempel Libicki, 2016; Rid, 2012). Offensive cyberoperasjoner som søker å ramme lukkede militære systemer, krever fysisk aksess (ved hjelp av innsidere, etterretningsoperatører eller uvitende aktører), skreddersydde cybervåpen som kan ramme det enkelte system, nøyaktige etterretninger om motstanderens systemer og sårbarheter samt teknologisk spisskompetanse om fiendens systemfunksjonalitet. Dette er naturlig nok ressurs- og tidkrevende. Vi har ikke inngående analyser som setter denne tid- og ressursbruken opp mot utviklingen av konvensjonelle våpen som kan utrette de samme effektene. Tilfellet Israel viser imidlertid at en småstat kan bli en cyberstormakt. Da kan det i prinsippet også gjelde for Norge.

Norges forsvarsevne bygger på NATO og troverdig alliert støtte. Vi kan med andre ord ikke analysere norsk offensiv opptreden isolert fra alliansen. I følge Foreign Policy har NATO nå tilrettelagt for offensive cyber operasjoner i rammen av alliansen (Ricks, 2017). Kapasiteten skal bestå i å tilrettelegge for kollektiv bruk av medlemslandenes offensive cyberkapabiliteter. Land som bidrar med egne kapabiliteter i en operasjon, vil beholde full kommando over både cybervåpen og styrker, til forskjell fra tradisjonelle operasjoner i rammen av NATO-alliansen. NATOs rolle vil i hovedsak være tilretteleggende og koordinerende. Denne kapasiteten kan være til nytte for Norge i væpnet konflikt og krig, og kan by på muligheter for tidlig alliert støtte. Et annet viktig aspekt ved NATOs nye offensive policy er at medlemsland som er store innen cybermakt kan bidra til kollektiv sikkerhet i alliansen uten å sette egne soldaters liv i fare. Utfordringer som må overkommes for at et slikt system skal kunne virke gjelder blant annet etterretning. Etterretningsdrevne cyberoperasjoner er engangsvåpen. Dersom en velger å delta med egne kapasiteter, mister en også aksess og muligheten til å bruke våpenet dersom egen suverenitet er truet. Å dele informasjon med allierte om at en har evne eller kapasitet til

[60] E-tjenestens operasjoner er sikkerhetsgraderte og omtales ikke videre i denne studien.

å utrette spesifikke effekter kan også bli avslørt for fienden og få sikkerhetspolitiske konsekvenser.

Uavhengig av NATOs tilretteleggende kapasitet og evne kan vi fastslå at offensiv opptreden ikke er et militært prinsipp anvendt av Norge i fredstid, hverken i eller utenfor cyberdomenet.

3.2.4 Oppsummering

Norge har ikke tydelige og enhetlige prinsipper for anvendelse av cybermakt. Det israelske prinsippet om enhetlig ledelse og mål kan ikke enkelt gjenkjennes i Norge, hvor ansvaret er spredt på flere departementer og med strategier som til dels har ulike målsettinger. Norsk strategisk styrkeøkonomisering finnes det både konsepter og strategier for, men hverken konsept eller strategi bidrar til å styrke norsk økonomi slik som i Israel. Offensiv opptreden i fredstid er ikke i tråd med småstatsrealismen og norsk overordnet politikk, og er følgelig heller ikke et konsept for norsk anvendelse av cybermakt. Offensiv opptreden bidrar ikke til forsvar, avskrekking og suverenitet i fredstid, slik som i Israel.

3.3 Delkonklusjon

De israelske målsettingene innen cybermakt er påvirket av Israels erfaringer med satsning på kvalitet fremfor kvantitet. Som en småstat med liten strategisk dybde har kvalitativ overlegenhet i form av høyteknologisk kampkraft kombinert med lang verneplikt vært en forutsetning for israelsk suksess i konflikter. Selv om Israel tidvis har vist at det har hatt for stor tro på teknologiens nytte, har det også vist evne til å tilpasse seg fortløpende. Israel er sterkt påvirket av trusselforståelsen og en kollektiv tradisjon. Israels historie med kollektive goder kan ha bidratt til samordning og enhetlig ledelse på cyberområdet. Det kan derfor tolkes som at det har vært nærliggende for Israel å satse så sterkt på cybermakt. I tillegg har Israel ved å etablere en *enhetlig ledelse* i cyberdirektoratet, ledet av PMO, evnet å få cybermaktens militære målsettinger til å passe inn med overordnede politiske *målsettinger*.

Når det gjelder styrkeøkonomisering, kan oppbyggingen av et militærindustrielt cyberkompleks bidra til å løse et av Norges største problem, nemlig at investering i militærmakt er en utgiftspost for staten – ikke verdiskapning? Det kan være mulig, men Israel er en nasjon hvis eksistens fortsatt anses som truet. Det samme trusselbildet gjelder ikke for Norge, og trusselpersepsjon påvirker forsvarsviljen. Israel har et forsvarsbudsjett på 4,7 % av BNP, mot Norges 1,6 av BNP (FN, 2018b). Trekker vi fra den reelle økonomiske verdiskapning fra cyberkomplekset er forskjellen mindre. Likevel: Enhver israeler er soldat og avtjener 3 års verneplikt, noe som også er en forutsetning for cyberkompleksets eksistens. Det samme har vi ikke i Norge. Tallenes tale er likevel klare: Israel styrker egen økonomi som en indirekte konsekvens av satsning på forsvar og cybersikkerhet.

Den mest påfallende forskjellen i israelsk og norsk sikkerhetsstrategi er at Israel med sin offensive opptreden søker å unngå krig gjennom avskrekking – deretter å vinne krigen dersom avskrekkingen feiler. Norge søker å hindre krig gjennom å balansere avskrekking og beroligelse, og hvis avskrekkingen feiler - å holde ut til allierte kommer til unnsetning. For Norge skyldes dette flere forhold, men mest av alt opplevelsen av fred og stabilitet i nærområdene. For Israel er situasjonen annerledes, noe som kan bidra å forklare at Israel har adoptert det militære prinsippet *offensiv opptreden* også for anvendelse av cybermakt i fredstid.

Vi kan oppsummere på følgende måte: Med bakgrunn i småstatsrealismen kan småstater som Israel og i prinsippet Norge være stormakter på enkelte områder – i dette tilfellet cybermakt. Men Israels bruk av offensiv cyber mot Irans atomvåpenprogram, som kan ha bidratt til israelsk avskrekking, kan også samtidig ha bidratt til et globalt rustningskappløp om cybermakt. Over tid kan derfor småstaten Israel miste sin posisjon som cyberstormakt, og miste sitt kvalitative fortrinn til fordel for teknologisk likeverdige og kvantitativt overlegne stater. Israels cybermakt med basis i offensiv opptreden *kan* derfor være et forbigående fenomen. Dette kan motvirkes gjennom innovasjon, hvor man sikrer seg forsprang overfor motstandere innen strategi og teknologi. Israel har lyktes med det – til nå. For Norges del er det i hovedsak organiseringen av *cyberdirektoratet* og prinsippene om *enhetlig ledelse og mål* og *strategisk styrkeøkonomisering* som kan være verdt en nærmere studie for eventuell adopsjon i fredstid. *Offensiv opptreden* er for Norge et mindre relevant verktøy for avskrekking, men mer relevant hvis avskrekkingen feiler, men det krever forberedelser i

fredstid. Forberedelser i fredstid krever både enhetlige mål og strategier og effektiv ressursutnyttelse – igjen en grunn til at cyberdirektoratet og cyberkomplekset er verdt et nærmere studium.

4 Tre scenarioer

For å vurdere om det er elementer ved israelsk cybermakt som kan bidra til å forbedre fremtidig norsk cybermakt har jeg utviklet tre typesituasjoner som jeg vil sjekke utvalgte karakteristika mot. Scenariene beskriver til sammen bredden av utfordringer et heldigitalisert samfunn og nettverksbasert forsvar må være forberedt på å møte i fred, krise og krig.

4.1 Scenario I – Forsvar

I dette scenariet trekkes Norge inn i stormaktenes rivalisering når konfliktene med Kina tilspisser seg og USA konsentrerer større deler av den militære innsatsen til Asia. Russland opptrer opportunistisk, presser frem egne regionale stormaktambisjoner på NATOs nordflanke og bruker digitale påvirkningskampanjer for å undergrave Norges legitimitet internasjonalt.

Den økte spenningen med NATO fører til at Russland setter indre del av bastionsforsvaret. NATO varsler store øvelser i Nord-Norge og havområdene rundt. Russland vil unngå å eskalere til en fullskala europeisk storkrig, og bruker sosiale media til fordekt organisering av store demonstrasjoner i flere europeiske NATO-land for å redusere sannsynligheten for alliert støtte til Norge.

Den økte russiske aktiviteten og aggressiviteten fører til at Norge svarer med å deployere majoriteten av landstyrkene nordover, mobiliserer Heimevernet, og bruke alle luft- og sjøstyrker for å maksimere avskrekking. Russland forstyrrer EKOM og navigasjons-,

posisjons- og satellitt-tjenester for å hindre norske militære operasjoner, og benekter samtidig kjennskap til den utstrakte digitale spionasjen som i lang tid har vært rettet mot norske sentrale myndigheter, beredskapsaktører, Forsvaret og kritisk infrastruktur.

NATO planlegger kollektivt forsvar av Norge og NATOs nordlige flanke, men artikkel 5 er ikke utløst.

Når den politiske spenningen tilspisser seg ytterligere, kommer det til trefninger mellom norske og russiske militære styrker i Finnmark. Russland påstår at Norge er aggressoren og hevder retten til selvforsvar. Cyberangrep mot lokale myndigheter og mediekanaler utfordrer Norges evne til å bevise det motsatte overfor egen befolkning og det internasjonale samfunn. Den russiske offensiven støttes av en stor elektronisk og digital kampanje, kombinert med fordekte kidnappinger og likvidasjoner, for å forstyrre Norges militære kommando- og kontroll-, sensor-, varslings- og våpensystemer. Utfordringen mot norsk forsvarsevne i det elektromagnetiske spektrum og cyberdomenet medfører tap på norsk side. Norge gjennomfører offensive cyberoperasjoner, støttet av enkelte alliansepartnere, mot russisk infrastruktur for å forstyrre russisk militær handlefrihet. Effekten av operasjonene er uviss.

Russland utvider cyberangrepene til større deler av landet og rammer sivile logistikk- og støttesystemer for å svekke norske styrkers utholdenhet. Det pågår mindre trefninger mellom russiske og norske landstyrker i lang tid før USA og enkelte NATO-land sender styrker til Norge. Mottak av alliert støtte forsinkes ytterligere av cyberangrep mot sivile logistikk- og støttesystemer, havner, flyplasser og jernbane.

I dette scenarioet møter Norge en motstander som utfordrer norsk kampkraft i det elektromagnetiske spektrum og digitale rom. Motstanderens evne til å gjennomføre digitale påvirkningsoperasjoner og digital sabotasje svekker norsk integritet, trekker konflikten ut og forsinker alliert støtte. Den norske balansen mellom avskrekking, offensiv opptreden og konflikteskalering påvirker de militære valgene, inkludert bruk av cybermakt.

4.2 Scenario II – Sikring av norsk suverenitet

I dette scenariet har de vestlige sanksjonene mot Russland svekket rubelen, og Russland fører en stadig mer aggressiv politikk for å utvide ressurstilgangen i sine nærområder. Russland krever større tilgang på naturressursene i nordområdene, mens Norge kjører en stram linje og spiller på FN-systemet, havretten, og avskrekking gjennom NATO-alliansen for å hevde norske suverene rettigheter og sikre økonomiske interesser.

Internett og sosiale media brukes til å gjennomføre fordekte påvirkningsoperasjoner for å undergrave Norges posisjon som fredsnasjon og menneskerettighetsforkjemper i det internasjonale samfunn og for å svekke Norges troverdighet i FN. Påvirkningsoperasjonene understøttes av intensivert russisk digital etterretning og forberedelser for sabotasje mot norsk maritim sektor, romsektor, olje- og gass, finanssektoren og sentrale myndigheter. Metodene er mer sofistikerte enn hva den enkelte sektor selv klarer å håndtere, og NSM og politiet har begrenset kapabilitet til å avhjelpe situasjonen. Flere av cyberangrepene kan attribueres til Kina, som kan ha interesse av at havretten utfordres.

Den russiske nordflåten endrer seilingsmønster og forsterker gradvis tilstedeværelsen i områdene rundt Svalbard. Den norske etterretningstjenesten fanger opp signaler om at Russland vil etablere en ny normaltilstand i nordområdene for å sikre egne økonomiske interesser over tid, men det er ingen signaler om at Russland vil eskalere til en åpen konflikt. Det forekommer gradvis hyppigere tilfeller av at russisk kystvakt hindrer norsk oppbringelse av den økende mengden utenlandske fartøy som bryter norsk lovgivning i vernesonen. I Norge tolkes handlingene som klare brudd på norsk territoriell integritet og suverene rettigheter. Forsvaret og Kystvaktens myndighetsutøvelse vanskeliggjøres av opportunistiske forstyrrelser på radar-, radio-, navigasjonssystemer og satellittbildetjenester. Norske myndigheter er tilbakeholdne med å offentlig attribuere påvirkningsoperasjonene, cyberangrepene og de elektroniske forstyrrelsene til Russland eller andre statlige aktører.

I dette scenarioet møter Norge store utfordringer med å sikre norske suverene rettigheter og økonomiske interesser. Det foreligger ingen etterretninger om at Russland har intensjon om å eskalere situasjonen til en militær konflikt, men norsk suverenitet brytes systematisk i sjø- og cyberdomenet. Norge møter store utfordringer med å håndtere den undergravende

virksomheten som foregår på sosiale media og opplever mindre aksept for det norske perspektivet i det internasjonale samfunn og FN.

4.3 Scenario III – Terrorisme og asymmetriske angrep

Innleide kontraktører som skal utføre arbeid på en norsk plattform, tar besetningen som gisler og truer med å sprenge plattformen dersom de ikke får innfridd sine krav om utvisning av en rekke muslimer fra Norge. Terroristene knyttes raskt til høyreekstreme miljøer som også har sterk tilknytning til lignende miljøer i Norden. Enkelte politikere er raskt ute med spekulasjoner om at Russland bruker høyreekstreme miljøer for å skape uro og splittelse.

Nyhetsbyråer og politiske partier til venstre blir rammet av mindre avanserte cyberangrep. Angrepene består for det meste av tjenestenektangrep og de-facing. I sosiale media blir terroraksjonen og cyberangrepene hyllet av høyreekstreme grupperinger i de nordiske landene.

Selv om PST og etterretningstjenesten avviser at det finnes signaler om at cyberangrepene var gjennomført av Russland, sår media tvil om norsk etterretning har tilstrekkelig grunnlag for vurderingene. I de kommende timene velger to store privateide offshore-selskaper å permittere russiske arbeidere av sikkerhetshensyn. I russiske media omtales saken som at Norge beskylder Russland for å stå bak terrorangrep og diskriminere russiske arbeidere.

Mens politiet med støtte fra Forsvarets spesialstyrker forbereder seg på å håndtere gisselsituasjonen, øker cyberangrepene i omfang og alvorlighet og rammer nå flere sektorer, nyhetskanaler og offentlige myndigheter. Kommunikasjon mellom myndighetene, media og befolkning vanskeliggjøres, og det er utfordrende for norsk kriseledelse å kunne håndtere situasjonen helhetlig. NSM og politiet ber om bistand fra Forsvaret.

I dette scenarioet eskalerer en «konvensjonell terroraksjon» til en uoversiktlig situasjon. Cyberangrepene er lite sofistikerte og av kort varighet, men vanskeliggjør kommunikasjon

med den norske befolkningen og det internasjonale samfunn. Det blir uklart om terroraksjonen er ledd i en fremmedstatlig kampanje eller gjennomført av ekstremister alene. Upresis informasjon og etterretning, samt manglende rammeverk for internasjonalt samarbeid om å håndtere cybertrusler blir en utfordring. Det uklare omfanget av situasjonen medfører usikkerhet om hvem som eier og bør håndtere krisen.

5 Konsekvenser for norsk cybermakt

I dette kapittelet analyseres norsk evne til *forsvar, suverenitetshevdelse og myndighetsutøvelse* i lys av scenarioene fra kapittel 4. De viktigste funnene oppsummeres og sammenlignes under hvert delkapittel med de mest relevante karakteristika fra israelsk cybermakt, for å belyse hvilken betydning disse kunne hatt for Norge.

5.1 Forsvar

Vi tar først for oss scenario I, hvor Norge møter en militært overlegen motstander som utfordrer norsk kampkraft i det elektromagnetiske spektrum og digitale rom. I dette scenarioet har Forsvaret med sin fremste oppgave å «forsvare Norge og allierte mot alvorlige trusler, anslag og angrep, innenfor rammen av NATOs kollektive forsvar» (Forsvarsdepartementet, 2016c, s. 23) den mest sentrale rollen, mens samfunnet for øvrig støtter.

I den innledende fasen brukes digitale påvirkningsoperasjoner, subversjon, for å undergrave norske interesser internasjonalt. Situasjonen oppleves som alvorlig, men ikke som en sikkerhetspolitisk krise. For småstaten Norge, hvor internasjonal legitimitet og støtte er sentralt, gis arbeidet med å kontre subversjonsvirksomheten høy prioritet. I Norge har hverken Forsvaret, NSM eller politiet fått tildelt et spesifikt ansvar for kontra-subversjon. Det at påvirkningsvirksomheten foregår delvis fordekt, men likevel med Russland som sannsynlig avsender, samt at aktivitetene stort sett foregår utenfor landets grenser, medfører at det blir

opp til regjeringens krisehåndteringssystem å håndtere dette. JD er lederdepartement, og KSE vil ha en sentral rolle for å støtte med å bygge et situasjonsbilde. Det norske krisehåndteringssystemet benyttes nasjonalt, men siden påvirkningen pågår utenfor Norge, vil UD også ha en sentral rolle for å håndtere undergravingen gjennom politiske og diplomatiske kanaler. E-tjenesten vil være en viktig aktør for å støtte norske krisehåndteringssystemet med etterretninger i dette arbeidet.

I neste fase av konflikten når bastionforsvaret settes, anses krisen som sikkerhetspolitisk, og FD tar over som lederdepartement. Kontrasubversjonsvirksomheten ute håndteres fortsatt av UD. Utfordringene med å håndtere subversjonsvirksomheten, samt tvil om Norges muligheter for å få alliert støtte, fører til at Norge innledningsvis frastår fra å mobilisere og velger beroligelse fremfor avskrekking. Cyberforsvarets fremste oppgave er å forsvare det norske forsvaret – for å bevare kampkraft og evne til avskrekking. I følge sjef Cyberforsvarets utsagn «holder vi ikke lenge». Evnen til å oppdage cyberangrep mot og i Forsvarets infrastruktur er for lav. Likevel: for at en motstander skal kunne ramme norske kampsystemer med digitale operasjoner, er han avhengig av å ha forberedt dette i lang tid i forveien. Slike forberedelser krever fysisk tilgang til lukkede systemer og etterretning utover cyberdomenet. Det er på ingen måte en umulighet, og selv om metodene er kostnads- og tidkrevende, er det ikke påvist at en slik angrepsvektor er mer krevende enn bruk av konvensjonelle våpen. Offensiv cybermakt kan ikke avvæpne denne type cybertrussel-aktører, og heller ikke avverge denne type angrep. Forebyggende sikkerhet og cyberforsvar kan, men Cyberforvarets manglende kapasitet kan føre til at Forsvarets evne til å maksimere avskrekking svekkes i kritiske perioder. På den annen side er det lite trolig at Russland vil benytte sine engangsvåpen før situasjonen eskalerer og det oppstår trefninger.

Når norsk avskrekking feiler, vil det å ramme norsk kampkraft med elektromagnetiske midler være et mer kostnadseffektivt og tilgjengelig alternativ enn digitale angrep. Som vist i analysen har Norge og NATO svært beskjedne midler for elektronisk beskyttelse og elektroniske mottiltak. Russland har på den annen side bygd opp denne kapasiteten over mange år. En detaljert beskrivelse av norsk forsvarsevne på dette området er sikkerhetsgradert, men vi kan nøye oss med å fastslå at russisk EK vil være et betydelig maktmiddel som kan degradere og forstyrre norske styrkers forsvarsevne. Forsvaret må i perioder kunne operere uten nettverksbaserte ild- og ledelsessystemer. Norske styrkers evne

til å operere på intensjonsbasert ledelse (som vist i blant annet Libya) har tidligere vist seg effektivt og kan oppveie for en del av forstyrrelsene, men ildledelse på tvers av innsatsrommet vil bli problematisk.

Dersom Russland har lykkes med å forberede digital sabotasje eller påvirkning av norske kampsystemer[61] og Cyberforsvaret ikke har evne til å oppdage dette, kan norske kampsystemer potensielt bli degradert. Det er sannsynlig at effektene vil være midlertidige og begrense seg til noen timer eller dagers varighet. Russland har demonstrert evne til å synkronisere effekter av digitale våpen i fellesoperasjoner, første gang i Georgia i 2008, deretter også i Ukraina og Syria. Den totale militære og sikkerhetspolitiske effekten av cybermakt kan således bli omfattende. Det vil være Cyberforsvarets oppgave å redusere skadeeffekter og tilgjengeliggjøre kampsystemene igjen. Kampsystemenes tilgjengelighet kan som oftest gjenopprettes hurtigere enn systemenes integritet og konfidensialitet. I et nettverksbasert forsvar hvor sensor, effektor og beslutningstaker er adskilt, og hvor både ildledere og våpenoperatører til syvende og sist skal utøve voldsmakt på vegne av staten, er både mellommenneskelig tillit og systemtillit en forutsetning for kampkraft. Gjenoppretting av kampsystemers integritet og konfidensialitet etter et kompromitterende cyberangrep vil derfor være tidkrevende fordi det handler om gjenoppretting av menneskelig tillit. Tvil om måldata, etterretninger og ordrers konfidensialitet og integritet vil kunne redusere operasjonstempo og handlekraft betraktelig og påføre Forsvaret unødvendige tap.

En indirekte metode med fordekte digitale angrep mot tredjepartssystemer som kan forstyrre norsk kampkraft, kan være enklere å gjennomføre enn digital sabotasje mot lukkede militære kampsystemer. Denne type forstyrrelser trenger heller ikke å være engangsvåpen. Systemer med grensesnitt til internett kan forstyrres med enklere metoder, for eksempel med tjenestenektangrep. NOUen *Digital sårbarhet - sikkert samfunn* har blant annet påvist svakheter i navigasjons- og satellittbildetjenester. Det er tjenester som norske kampsystemer på ulike nivå og i ulik grad benytter seg av. Analysen har vist at det er NSM som har det overordnede ansvaret for forebyggende sikkerhet nasjonalt, men at tilslutning til VDI fortsatt er frivillighetsbasert. Ved digitale angrep mot sivil infrastruktur er det den enkelte virksomhet selv som er ansvarlig for å beskytte, gjenopprette og også å forsvare seg mot fremmedstatlig

[61] For eksempel slik som Israelske droner og F-16 har blitt utsatt for tidligere (se BBC, 2016).

sabotasje. I et scenario som dette vil Forsvaret ikke ha kapasitet til å støtte sivile virksomheter. I Ukraina ble sivilt personell med ansvar for drift av kritiske funksjoner utsatt for likvideringer og kidnappinger. Et slikt operasjonsmodus kan ikke ses bort fra blir brukt også i et scenario som dette. Sivile IKT-driftsmiljøer med ansvar for opprettholdelse av kritisk cyberinfrastruktur som kan påvirke forsvarsevnen, må antas å være spesielt utsatt. Det vil være en politioppgave å beskytte disse – også i krise og krig. Et spørsmål som krever en dypere studie, blant annet av krigspsykologi, er om sivile aktører har vilje til å stå i en slik situasjon. Vi har ikke empiri for å hevde hverken det ene aller andre.

E-tjenesten, som har ansvaret for offensive cyberoperasjoner, kan når operasjoner er forberedt, gjennomføre digitale motangrep mot utvalgte mål. Norge kan også anmode om tidlig alliert støtte (se kapittel 3.2.3) i form av offensive cyberangrep for å oppnå ønskede effekter. For Norge og NATO's del gjelder den samme logikken som omtalt for Russland: effektene av cyberangrepene vil ha størst virkning når synkronisert i tid og rom med den fellesoperative innsatsen.

Når Russland utvider cyberangrepene til å ramme sivile systemer som understøtter Forsvaret, vil NSM, SRMene og den enkelte virksomhets evne og vilje være av kritisk betydning for Forsvarets utholdenhet og evne til mottak av alliert støtte. Virksomhetene må være trent og erfarne i å forebygge, beskytte, skaderedusere og gjenopprette hurtig etter digitale angrep. Elektroniske og elektromagnetiske angrep vil også kunne bli benyttet mot det sivile støtteapparatet, spesielt mot sjø- og luftfart. Her har ikke NSM et ansvar, men Nkom. Nkom har ikke relevante virkemidler for å møte denne type trussel. Cyberforsvaret eller politiet vil ikke kunne støtte virksomhetene i denne situasjonen.

NSM NorCERT har begrenset evne til å støtte alvorlige digitale angrep som treffer flere sektorer samtidig. Støtten vil i hovedsak være begrenset til distribusjon av et felles situasjonsbilde og rådgivning overfor SRMer og virksomheter som allerede er del av VDI. Større norske virksomheter som også leverer tjenester bredt til samfunnet og internasjonalt, vil ha en egeninteresse i å holde egne systemer intakte, og derfor sannsynligvis bruke betydelige midler på egenbeskyttelse og cybersikkerhet. Mindre nasjonale og internasjonale virksomheter kan finne det tryggere og enklere å trekke seg ut av konfliktsonen, eller fra forholdet til Norge eller Forsvaret, for å redusere egen risiko for å bli angrepet eller påvirket.

Dette vil være avhengig av virksomhetenes egen kostnytte-kalkyle – private foretak opererer tross alt i konfliktsoner rundt om i verden. Med mangelen på god empiri fra åpne kilder fra tidligere konflikter er det ikke mulig å fastslå om virksomheter som er ansvarlige for å beskytte kritisk infrastruktur (som både forsvarsevne og mottaksapparat er avhengig av), faktisk vil være kapable til å forsvare seg selv mot fremmedstatlige cyberangrep. Det vi derimot kan slå fast, er at Forsvaret og dermed statssikkerheten er avhengig av at de ansvarlige virksomheter utviser både vilje og evne til digitalt selvforsvar mot fremmedstatlige militære aktører.

Oppsummering

I tidlig fase hvor Norge utsettes for politisk press og internasjonal undergravende virksomhet ved hjelp av digitale virkemidler, har hverken Forsvaret, NSM eller politiet ansvar for kontra-subversjon. I Israel håndteres kontrasubversjon av ISA. Operasjoner for å kontre subversjonsvirksomhet utenfor Israel ville vært gjenstand for politisk styring. Israel som forholder seg til denne oppgaven til daglig har både erfaring og etablerte rutiner for å håndtere subversjon.

I tidlig fase er defensiv cybermakt det viktigste middelet for å sikre kampstyrkenes handlefrihet og dermed Forsvarets evne til å maksimere avskrekking. Cyberforsvaret er i henhold til eget utsagn ikke i stand til å sikre handlefrihet i cyberdomenet. C4iCDD er i henhold til israelske utsagn øvd og i stand til å beskytte egne styrkers kampkraft mot fiendtlige digitale angrep (Opall-Rome, 2017) og vil således ikke stå overfor en utfordring av samme dimensjon.

Hvis avskrekkingen feiler, vil russisk EK være den største trusselen mot norske kampsystemer. Forsvaret har begrenset beskyttelseskapasitet på dette området. Også IDF har måttet klare seg i perioder uten kommunikasjon, noe de blant annet opplevde i Gaza-krigen. Oppdragsbasert ledelse og ordonnanser var løsningene på utfordringene den gang (Lapid & Gilboa, 2012). Ordonnanstjeneste løser derimot ikke utfordringer med å engasjere ild på tvers av innsatsrommet for Norge.

Kritisk sivil infrastruktur og funksjoner som skal understøtte kampkraft, utholdenhet og mottak av allierte, er mer sårbare og enklere mål enn militære lukkede systemer og trenger beskyttelse i alle faser. Det kan sås tvil om sivile IKT-avdelinger er i stand til å beskytte seg mot fremmedstatlig digital sabotasje fra en stormakt. Den samme logikken gjelder for Israel, men i Israel er all kritisk infrastruktur beskyttet av CERT-IL. Israel er således bedre rustet for å bevare både kampkraft og utholdenhet.

Offensive cyberoperasjoner i rammen av kollektivt forsvar av Norge kan i prinsippet følge samme logikk som for Russlands del og ramme russisk utholdenhet i tidlig fase – allerede før alliert støtte ankommer Norge. Israel ville ha benyttet offensiv cybermakt for å frata motstanderen initiativ i tidlig fase og helst før trusselen manifesterte seg.

5.2 Suverenitet

Her drøftes scenario II, hvor Norge møter utfordringer med å sikre norske suverene rettigheter.
I første fase, hvor Norge blir utsatt for digitale påvirkningsoperasjoner, gjelder samme forklaring som i forrige del – kontrasubversjon må først og fremst håndteres politisk, men kan delegeres. Subversjonsvirksomheten er mindre åpenlys, og fordi det ikke finnes en identifisert aktør i staten som har ansvaret for kontrasubversjon, tar det tid lang tid å skaffe informasjon som positivt kan attribueres til en aktør. I denne situasjonen vil sannsynligvis Etterretningstjenesten få oppdrag om å støtte myndighetenes håndtering. Selv om PST og NSM har et innenriks ansvar, har de begge internasjonale samarbeidsavtaler og kanaler som kan bidra til etterforskning og attribusjon av subversjonsvirksomheten. Det er også mulig at PST kan bli bedt om å lede arbeidet[62] gjennom FKTS.[63]

Den intensiverte digitale etterretningen kan ta lang tid å oppdage. Det skyldes delvis at mange av de utsatte virksomhetene og forvalterne av kritisk infrastruktur ikke er del av VDI, og

[62] Politiets overvåkingstjeneste (POT) hadde tidligere ansvaret for kontra-subversjon.

[63] Felles kontraterrorsenter

delvis at en del av de private aktørene ikke ønsker å rapportere angrep til NSM eller politiet av hensyn til kunder og aksjekurser. Det vil i tillegg ta lang tid å positivt attribuere de mange angrepene som faktisk blir oppdaget, og det kan være utfordrende å se sammenhengen mellom mange angrep hvis signaturer og fremgangsmåte er ulike. NSM, politiet og E-tjenesten vil kunne ha fordel av at informasjonen blir offentlig kjent slik at flere virksomheter skjerper rapporteringsrutinene. Fordi flere av inntrengningene ser ut til å komme fra Kina, mens den den sikkerhetspolitiske situasjonen og subversjonsvirksomheten peker mot Russland, holder myndighetene tilbake attribusjon av etterretningsoffensiven. Konsekvensen er at virksomheter og forvaltere av kritisk infrastruktur som ikke er medlem av VDI, ikke oppdager at de er utsatt for etterretning og forberedelser på sabotasje. Forsvarssektoren, politiet og alle SRMer vil likevel bli rutinemessig informert og ha mulighet til å iverksette tiltak i egne sektorer. Den økte mengden cyberangrep representerer en endring i normalsituasjonen, men siden både omfang og alvorlighet tar lang tid å avdekke, oppfattes sannsynligvis ikke angrepene som brudd på norsk suverenitet.

FOH vil med bakgrunn i jevnlige situasjonsoppdateringer med POD og NSM ha mulighet til å se cyberhendelsene i sammenheng med Nordflåtens endrede seilingsmønster og overordnet militært situasjonsbilde. NSM og POD vil på samme måte ha muligheten til å koble hovedlinjer i russisk militær aktivitet opp mot aktivitetene i det sivile cyberdomenet. Evnen til å oppdage endring i normalsituasjonen i flere domener samtidig vil være viktig for både forsvars og justissektoren, og muliggjør også en helhetlig rapportering til strategisk og politisk ledelse.

Selv om Russland i 2008 brukte cyberoperasjoner for å forme stridsmiljøet i døgnene før land-, luft- og sjøstyrker ble satt inn i Georgia-konflikten (se Hollis, 2011), har E-tjenesten i denne situasjonen etterretninger som tilsier at Russland ikke er interessert i å eskalere situasjonen til en åpen konflikt. Det er for øvrig også lite som tilsier at Russland vil gjøre som det har gjort tidligere, siden det har valgt forskjellig modus operandi i alle konflikter siden 2008. Norske myndigheter vil likevel oppfatte å stå i en presset situasjon hvor både suverene rettigheter og norske økonomiske interesser oppleves truet. Russland har hverken mobilisert styrker eller truet med bruk av militær makt, men Norge er kjent med den russiske ambisjonen om å sikre seg økt fotfeste og ressurstilgang i nordområdene. Norge opplever å stå i en gråsone på vei inn i en langvarig sikkerhetspolitisk krise. Cyberforsvarets ressurser vil ikke

bli utnyttet til å støtte sektorvise responsmiljøer eller virksomheter som ikke er i stand til å håndtere egen beskyttelse, men holdes i beredskap til nytte for Forsvaret i tilfelle en eskalering av konflikten. NSMs rolle er desto viktigere.

Situasjonen forverres når det etter hvert forekommer hyppige tilfeller av at russisk kystvakt bryter norsk suverenitet, samtidig som det oppleves hyppige forstyrrelser på radar-, radio-, navigasjonssystemer og satellittbildetjenester. Forstyrrelsene er primært rettet mot norske militære fartøy, tjenester og systemer, men påvirker også sivil luft- og sjøfart. Forsvaret har begrensede militære innsatsmidler som kan motvirke forstyrrelsene, men har alternative frekvenser og utstyr som kan bidra til at nødkommunikasjon opprettholdes mellom styrkeelementer og operativ ledelse, riktignok med forringet situasjonsforståelse og dertil nedsatt beslutningstempo hos fellesoperativ, strategisk og politisk ledelse. Nkom kan bidra med spektrumanalyser og peiling for å fastslå opprinnelsen til forstyrrelsene, men har ikke myndighet til å gjøre noe med utstyr som ikke befinner på norsk territorium.

Offensiv cybermakt kan i teorien også brukes av Norge i en situasjon hvor norsk suverenitet trues. Det er imidlertid uklart om dette vil ha noen gevinster utover tradisjonell etterretning.

Oppsummering

Når Cyberangrep rammer tverrsektorielt, vil det være utfordrende for NSM NorCERT å støtte flere sektorer, med mindre angrepene er av lik karakter og kan håndteres likt i alle sektorer. Utfordringen gjelder i enda større grad for CERT-IL som selv skal beskytte all kritisk infrastruktur. Cyberforsvarets kapasiteter vil ikke kunne støtte sivile virksomheter i en situasjon hvor norsk suverenitet trues. Selv om C4iCDD angivelig skal kunne forsvare utvalgt sivil kritisk infrastruktur er det uvisst om dette kan bidra til å sikre suverene rettigheter i større grad enn i Norge.

Evne til å forstå normalsituasjonen i alle domener, også cyberdomenet, er nødvendig for både militær og sivil ledelse for å kunne velge begrunnete handlemåter i gråsoner. Samarbeidet mellom FOH, politiet og NSM/FCKS bidrar til dette, men situasjonsforståelsen er fortsatt begrenset uten DGF og evne til tidlig varsling. Selv om analysen ikke har påvist at Israel har DGF-lignende løsninger, er det totale informasjonstilfanget fra både CERT-IL og

etterretningstjenestene større. Den sentrale samordningen kan sammen med dette potensielt bidra til at Israel har bedre forutsetninger for å etablere en helhetlig situasjonsforståelse.

Offensiv cybermakt er et mindre relevant virkemiddel for å beskytte norske suverene rettigheter. For Israels del ville offensive cyberangrep kunne bli benyttet på samme måte som i en væpnet konflikt. Israel ville i tillegg kunne benyttet seg av digitale forkjøpsangrep for å sikre egen suverenitet.

5.3 Myndighetsutøvelse

Her behandles scenario III, hvor en terroraksjon eskalerer og utfordrer norsk kriseledelse.
I aksjonenes innledende fase er det liten tvil om at terrorsituasjonen må behandles av justissektoren og politimyndigheter. Fordi situasjonen foregår på norsk sokkel, blir Forsvaret ganske umiddelbart anmodet om å bistå og forberede spesialstyrker og overvåkningskapasiteter til støtte for politiet. Siden politiet har svært begrensede ressurser for å håndtere cyberangrep blir Forsvaret også anmodet om å støtte med Cyberforsvarets ressurser. Forsvaret oppfatter på dette tidspunkt situasjonen som en terroraksjon, kombinert med sporadiske cyberangrep, og FOH forbereder derfor Cyberforsvaret på å støtte kriseledelsen. Som tidligere analyse har påpekt, vil det være begrenset hva Cyberforsvaret kan støtte med, spesielt i infrastruktur hvor det ikke har operert tidligere.

Den uklare situasjonen bidrar til uklarhet om hvem som eier krisen. Dette kan potensielt føre til at Forsvaret velger å holde tilbake støtte fra Cyberforsvaret, og heller ha Cyberforsvarets mobile enheter på beredskap i tilfelle krisen er mer alvorlig enn først antatt. Valget kan da heller falle på en mer avgrenset form for støtte, i form av rådgivning og spesialistkompetanse på utvalgte områder.

NSM NorCERTs rolle vil også i dette scenarioet være en sentral aktør for å støtte KSE og kriseledelsen med å etablere en helhetlig situasjonsforståelse. NSM NorCERT på sin side vil være avhengig av samarbeid med de enkelte sektorer og virksomheter så vel som politiet og

E-tjenesten for å forstå helhetsbildet. I dette vil FCKS være et viktig ledd. I tillegg vil samarbeid mellom FCKS og FKTS være viktig.

DGF er et verktøy etterlyst av E-tjenesten for å kunne oppfylle sitt oppdrag. DGF kan potensielt ha gode effekter rettet mot terrorisme og for tidlig varsling av (både mer og) mindre sofistikerte cyberangrep. Etterretningstjenesten vil være en av de viktigste støttespillerne til NSM, Forsvaret, politiet, PST og kriseledelsen for å forstå den grenseoverskridende situasjonen, men vil i mangel av et DGF være prisgitt samarbeid med andre lands etterretningstjenester.

Oppsummering

Uklarhet om hvem som eier krisen er ingen ny problemstilling i norsk sammenheng. Det er nærliggende å anta at Israels MoD vil ivareta krisehåndteringen på et tidligere stadium enn i Norge, med bakgrunn i Israels trusselpersepsjon og militære tradisjon.[64]

I Norge vil det være opp til den enkelte virksomhet og SRM med støtte fra NSM NorCERT å håndtere cyberangrepene, uavhengig av hvem som eier krisen. For Israels del er de to organene som er ansvarlige for å håndtere terrorisme og cyberangrep direkte underlagt PMO. Cyberdirektoratets NCSA vil håndtere cyberangrep mot sivil sektor og ISA har hovedansvaret for å håndtere terrorisme uavhengig av om krisen er sikkerhetspolitisk. Politiets rolle i håndteringen av cyberangrepene vil være reaktiv også i Israel. For både Norge og Israels del kan det sås tvil om Cyfor og C4iCDDs relevante kapasitet til å støtte håndteringen av cyberangrepene mot sivil sektor. Israels cyberkompleks har ingen rolle innen myndighetsutøvelse eller krisehåndtering men vil kunne bidra til at nye og ukjente cybersikkerhetsutfordringer raskere lokaliseres og løses. E-tjenestens bidrag for å forstå helhetssituasjonen vil være viktige, men begrenset av manglende tilgang til data gjennom DGF. Israel har på sin side har et større etterretnings og overvåkningsapparat og vil med basis i sin erfaring trolig kunne etablere helhetsoversikt og håndtere situasjonen raskere.

[64] I Israel er beredskaps og krisefunksjoner som tidligere lå under «National Emergency Management Authority» (sammenlignbart med DSB) i dag en del av IDF (Housen-Couriel, 2017, s. 14).

6 Konklusjon

Svaret på problemstillingene jeg har analysert i denne studien er som følger:

Det som kjennetegner israelsk cybermakt er primært at Israel bruker cybermakt aktivt og offensivt i fredstid for å unngå krig, samtidig som cybermakt anvendes for å styrke israelsk økonomi. Offensiv cybermakt brukes målrettet for skjult ødeleggeleggelse av fiendtlige initiativ og for å bidra til å akkumulere avskrekking. Israelsk cybermakt er til for statens overlevelse. Det som kjennetegner norsk cybermakt er heller oppfattelsen av avmakt og manglende evne til å ivareta stats- og samfunnssikkerheten uten at dette går utover individuelle demokratiske rettigheter. Norsk fokus ligger ikke på statssikkerheten, men på IKT-sikkerhet og samfunnsøkonomi.

De viktigste likhetene er at Norge og Israel besitter stort sett de samme organisatoriske enhetene som kan bidra til cybermakt. Og videre at begge land i prinsippet deler noen grunnleggende forutsetninger for å oppnå cybermakt. Begge er høyt digitaliserte samfunn med en høyt utdannet befolkning, og begge har høyteknologiske forsvar. Norsk myndighetsutøvelse står heller ikke tilbake for Israel selv om organiseringen har ulikheter. Studien har vist at med bakgrunn i småstatsrealismen kan småstater som Israel, og i teorien Norge, være cyberstormakter.

De viktigste forskjellene er at Israels sentralstyrte cyberdirektorat tilrettelegger for en enhetlig cyberpolitikk og at det er en tydelig rød tråd fra politikk til militær strategi – i Norge mangler det en enhetlig ledelse av cyberpolitikken og den den råde tråden fra cyberpolitikk til militær strategi er lite synlig. Israels militærindustrielle cyberkompleks bidrar til en nasjonal styrkeøkonomisering som øker statens overlevelsesevne ved å forsterke israelsk økonomi og forsvarsevne – noe sammenlignbart finnes ikke i Norge.

Når det gjelder den tredje og mest dyptgripende problemstillingen, nemlig hvilke erfaringer som kan hentes fra Israels cybermakt for fremtidig utvikling av norsk cybermakt, er svaret noe mer komplekst. Basert på analysen av norsk og israelsk organisering og prinsipper for

cybermakt, samt beskrivelsen av norsk evne til anvendelse av cybermakt i de tre scenarioene, skal vi drøfte enkelte karakteristika knyttet til israelsk cybermakt som potensielt kan anvendes for å endre norsk avmakt til norsk cybermakt. Det første punktet er av overordnet karakter, og har implikasjoner for de mer spesifikke punktene som følger.

Tradisjon og trussel

Både Israel og Norge er småstater i tradisjonell forstand. Ulike forhold fører likevel til at Israel anses som en cyberstormakt. Den mest grunnleggende årsaken til at Israel har utviklet en særlig kapasitet på dette området handler om tradisjon og trussel. *Trusselen* oppfattes som eksistensiell. Israel har lært seg å leve med spørsmålet om overlevelse som vedvarende problem, og å forsvare seg med alle midler, om nødvendig alene. Dette er et ganske annet utgangspunkt enn Norge, som til tross for økende utfordringer, fortsatt lever i en slags tilstand av «dyp fred». Norge har derfor ikke like sterke incentiver til å utvikle alle former for virkemidler som kan styrke landets evne til avskrekking og forsvar, herunder potensialet i å bygge seg opp som en cyberstormakt.

Selve maktapparatet i Israel er også sterkt påvirket av trusselforståelsen, samt en *kollektiv tradisjon*. Israels historie med kollektive goder, nøret opp under av en felles utenforstående trussel, vil kunne sies å ha bidratt til den sterke samordningen og enhetlige ledelsen i israelsk politikk på en rekke områder, herunder cyberområdet. Dette skiller seg fra Norge som har en mer fragmentert tradisjon. Riktignok har også Norge en lang historie med tett sivilmilitært samarbeid, herunder gjennom totalforsvaret, men også det forble sterkt fragmentert gjennom hele den kalde krigen.

Implikasjonene av dette for Norge og norsk cybermakt er at det er så grunnleggende forskjeller mellom israelsk og norsk tradisjon og trusselpersepsjon at det er lite som tyder på at Norge kan oppnå samme utvikling på cyberområdet som Israel. Samtidig vil det være enkelte områder der Norge *kan* trekke på erfaringer fra Israel, dog uten å gå like langt som dem.

Felles mål og enhetlig ledelse

Israel har ved å etablere en *enhetlig ledelse* i cyberdirektoratet evnet å få cybermakten til å passe inn med sine overordnede politiske *målsettinger*. Dette har de klart selv uten en å

formulere en cyberstrategi. I Norge har vi en rekke strategier med til dels sprikende målsettinger. For eksempel er det få sikkerhetspolitiske målsettinger som farger norsk IKT-, cyber-, eller digitaliseringsstrategi, selv om alle er enige i at sårbarhetene har konsekvenser for både samfunns- og statssikkerheten. Denne analysen har vist at det israelske cyberdirektoratet har samlet oppgaver som i Norge er fordelt på en rekke direktorater. En fusjonering av ansvarsområder også i Norge kan føre til en mer enhetlig ledelse og felles målsettinger hvor både sikkerhetspolitikk, digitalisering og samfunnsøkonomi kan møtes. En vil da måtte vurdere sammenslåing under ett departement deler av DSB, Nkom, Datatilsynet, Difi, KUD og NSM og muligens flere aktører.

Strategisk styrkeøkonomisering

En av de største sikkerhetspolitiske utfordringene for Norge er at forsvar anses som en utgiftspost, og ikke en verdi. Dette er ikke unaturlig for et land i et fredelig hjørne av verden. Men som demonstrert i Ukraina i 2014 kan det sikkerhetspolitiske bildet endres raskt. Israel har gjennom det militærindustrielle cyberkomplekset evnet å få investering i forsvarsevne til å bli en av statens viktigste inntektskilder. Cyberkomplekset fronter i dag Israels økonomiske vekst og bidrar samtidig til både samfunns- og statssikkerheten. Er det mulig å få til noe lignende i Norge? Norge deler en del forutsetninger for en slik mulighet med Israel. Både Norge og Israel er blant verdens mest digitaliserte samfunn, har god økonomi og en høyt utdannet befolkning. Men det er en forutsetning for komplekset vi ikke deler: Unit 8200 og C4iCDD styrkeproduserer cyberspesialister målrettet til cyberkomplekset. Dette er mulig for IDF fordi de får igjen for det i det lange løp. IDF høster teknologiske løsninger, taktikk og strategi fra komplekset. Skulle vi gjort noe lignende i Norge, ville det krevd at både E-tjenesten og Cyberforsvaret tok inn et høyt antall vernepliktige. Dette vil kreve en holdningsendring i begge leire. Forvaret ville også måtte endre sin rekrutterings- og ansettelsesstrategi, og innføre incentiv-ordninger som ikke finnes i dag.

Cyberkomplekset styrker Israels forsvarsevne og bidrar samtidig til å styrke økonomien, og kan være verdt en nærmere studie for Norge – da med fokus på norske sikkerhetspolitiske interesser – for eksempel cybersikkerhet i nordområdene, for maritim sektor, olje- og gassnæringen, samt løsninger for det globale markedet som møter det demokratiske dilemma og samtidig understøtter norsk småstatsrealisme: demokratiske rettigheter og en stabil

internasjonal rettsorden. CCIS på Gjøvik er i dag et mikrokompleks som kunne vært basis for etablering av et større kompleks.

Cyberforsvar

Defensiv cybermakt er det viktigste middelet for å sikre norske kampstyrkers handlefrihet og dermed Forsvarets evne til å maksimere avskrekking. Cyberforsvaret er i henhold til eget utsagn ikke i stand til å sikre handlefrihet i cyberdomenet. Denne studien har strengt tatt ikke påvist annet enn det sjef Cyfor har uttalt offentlig, men har synliggjort at cyberforsvarets manglende evne kan få følger for statssikkerheten. I Israel har angivelig C4iCDD fått et ansvar for forsvar av utvalgt kritisk infrastruktur. Cybermilitær støtte til forsvar av sivil kritisk infrastruktur har blitt fremhevet som utfordrende og mangelfull i både Israel og Norge – først og fremst fordi digitale forsvarsoperasjoner krever inngående kunnskaper om og kjennskap til både infrastrukturen og virksomhetsprosessene den skal understøtte. En ordning slik som i Israel vil være lite aktuelt for Norge: For det første fordi Cyfor ikke er dimensjonert for å støtte sivile. For det andre fordi det vil kreve tilstedeværelse eller overvåkning mer eller mindre kontinuerlig, og siden IKT-sikkerhet ikke kan frakobles helt fra cyberforsvar vil slik organisering gå på tvers av ansvarsprinsippet.

I Norge er det den enkelte virksomhet som har ansvaret for å beskytte kritisk infrastruktur, uavhengig av infrastrukturens verdi for staten, trusselen, og sårbarheten. I Israel er CERT-IL tillagt de samme oppgaver som NSM NorCERT – monitorering og koordinering – men i tillegg beskyttelse av all kritisk infrastruktur. Denne studien har gitt indikasjoner på at den israelske modellen kan være mer fordelaktig enn den norske, spesielt i krise og krig. Dog vil også NSM NorCERT stå overfor lignende problemstillinger som beskrevet over om Cyberforsvaret knyttet til behovet for kontinuerlig tilstedeværelse og overvåking av og i kritisk infrastruktur, om det skulle gjennomføres. Informasjonssikkerhet og grunnsikring vil alltid være virksomhetens ansvar. Men det mest sentrale poenget belyst i studien er at Forsvarets evne til å ivareta statssikkerheten er avhengig av at sivil kritisk infrastruktur forsvares mot digitale angrep i fred, krise og krig.

Offensiv opptreden

I Israel er offensiv opptreden mellom kriger viktig for å unngå krig og akkumulere avskrekking. For Norge er offensiv opptreden i fredstid mindre relevant, i sikkerhetspolitiske kriser og krig desto mer relevant. I Israel er offensiv cybermakt en integrert del av militær doktrine, og tilsynelatende også av fellesoperativ innsats. Israels offensiv er muliggjort av flere faktorer, blant annet cyberkomplekset, som bidrar med å utvikle teknologi og cybervåpen. Norsk forsvarsevne er fundamentert i NATO-alliansen, det kan en økt satsning på offensiv cybermakt for å kontre russiske kapabiliteter i tidlig konfliktfase også være.

Samlet konklusjon – Kan Norge bli en cyberstormakt?

Norge har mye å lære ved å studere israelsk cybermakt, men ikke alt er relevant eller formålstjenlig. Prinsippet om offensiv opptreden i fredstid, passer ikke med norsk småstatsrealisme og sentralisert forsvar av kritisk infrastruktur bryter med ansvarsprinsippet. Derimot så kan det være helt innenfor måls rekkevidde å etablere felles målsettinger som bidrar til statssikkerhet, samfunnsøkonomi og demokrati. En enhetlig ledelse på cyberområdet vil kreve at deler av flere direktorater samordnes under ett departement. En strategisk styrkeøkonomisering lik den som finnes i Israel er ikke realistisk oppnåelig med dagens vernepliktsordning. En strategisk styrkeøkonomisering i mindre skala som fremmer norske interesser kan likevel være mulig dersom Norges forsvars- utenriks- og sikkerhetspolitiske målsettinger møter norske økonomiske målsettinger. Men i dette kan ikke Norge forvente å oppnå annet mindre effekter, fordi Israels kvalitative overlegenhet muliggjøres gjennom lang verneplikt, vel så mye som i overlegen teknologi. At Forsvaret ikke er i stand til å beskytte seg selv mot fremmedstatlig cybermakt er mulig å endre på, men krever målrettet investering i digitale og elektromagnetiske beskyttelsestiltak som kan håndtere truslene. Cyberforsvaret, NSM eller politiet kan ikke forsvare sivil kritisk infrastruktur. Sivile virksomheter må derfor selv være i stand til å beskytte seg mot fremmedstatlige cybertrussel-aktører. Dette er mulig med en videreutvikling av NSM NorCERT og VDI som inkluderer at alle samfunnskritiske verdier.

Studien har vist at det *ikke* er realistisk at Norge kan bli en cyberstormakt som Israel, fordi offensiv opptreden i fredstid ikke er forenelig med norsk politikk, og fordi strategisk

styrkeøkonomisering med basis i Forsvaret ikke er realistisk oppnåelig. Norge *kan* derimot snu avmakt til cybermakt. Dette kan først og fremst skje ved at norsk politikk på cyberområdet forenes med sikkerhetspolitiske målsettinger. Dernest ved at det investeres i sivil og militær cyberforsvarsevne som sikrer opprettholdelse av fellesoperativ kampkraft, utholdenhet og alliert mottak. Og sist men ikke minst ved satsing på alliert cybermakt som kan kontre motstanderes evne til å forstyrre handlefrihet og redusere utholdenhet allerede i tidlig konfliktfase.

7 Litteraturliste

33rd Government of Israel. (2015a). Government Resolution No. 2443 of February 15, 2015: Advancing National Regulation and Governmental Leadership in Cyber Security. Hentet 18. september 2017, fra https://ccdcoe.org/sites/default/files/documents/Government Resolution No 2443 - Advancing National Regulation and Governmental Leadership in Cyber Security.pdf

33rd Government of Israel. (2015b). Government Resolution No. 2444 of February 15, 2015: Advancing the NAtional Preparedness for Cyber Security. Hentet 18. september 2017, fra https://ccdcoe.org/sites/default/files/documents/Government Resolution No 2444 - Advancing the National Preparedness for Cyber Security.pdf

Anderson, C., & Sadjadpour, K. (2018). *Iran's Cyber Threat: Espionage, Sabotage, and Revenge*. Washington DC. Hentet fra http://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

Aron, R. (1966). *Peace and War. A Theory of International Relations*. London: Weidenfeld and Nicolson.

Askvik, Ø. (2015). *Utvikling av langtrekkende konvensjonelle presisjonsvåpen – konsekvenser for Norges evne til avskrekking og forsvar mot angrep*. Forsvarets høgskole.

Baram, G. (2017). Israeli Defense in the Age of Cyber War. *Middle East Quarterly*, *24*(1), 1–10. Hentet fra http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=120333319&site=ehost-live

BBC. (2016, januar 29). US and UK «hacked into Israeli drones and planes». *BBC News*. Hentet fra http://www.bbc.com/news/world-middle-east-35440523

BBC. (2017, desember 19). Cyber-attack: US and UK blame North Korea for WannaCry. Hentet fra http://www.bbc.com/news/world-us-canada-42407488

Ben-israel, I., & Tabansky, L. (2011). An Interdisciplinary Look at Security Challenges in the Information Age. *Military and Strategic Affairs*, *3*(3), 21–37.

Berg, O. T. (2018). Politikk. I *Store norske leksikon (2018, 20. februar)*. Hentet fra https://snl.no/politikk

Cate, F. H., & Dempsey, J. X. (2017). *Bulk Collection: Systematic Government Access to*

Private-sector Data. Oxford: Oxford University Press.

CCIS. (2018). *Årsrapport 2017 for NTNU Center for Cyber and Information Security*. Hentet fra https://www.ntnu.edu/documents/1269858715/1278988725/NTNU+CCIS+2017.pdf/aec1871d-9806-4a49-b9bc-c05c046d90d2

Chekinov, S. G., & Bogdanov, S. A. (2013). The Nature and Content of a New-Generation War. *Military Thought*, (4), 12–23.

Clark, C. (2016, juli 15). BAE Systems Inches Out In Public On Electronic Warfare. *Breakingdefence.com*. Hentet fra https://breakingdefense.com/2016/07/bae-systems-inches-out-in-public-on-electronic-warfare/

Cyberspark. (2018). Cyberspark - Israeli innovation arena. Hentet 28. april 2018, fra http://cyberspark.org.il/

DeNardis, D. L., & Raymond, M. (2013). Thinking Clearly About Multistakeholder Internet Governance. *SSRN Electronic Journal*, 1–18. http://doi.org/10.2139/ssrn.2354377

Departementene. (2012). Nasjonal strategi for informasjonssikkerhet. Oslo: Fornyings-, administrasjons- og kirkedepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikker/id710469/

Direktoratet for samfunnssikkerhet og beredskap. (2015). Departementenes systematiske samfunnssikkerhets- og beredskapsarbeid. DSB. Hentet fra http://www.dsbinfo.no/DSBno/2015/Tema/Departementenessystematiskesamfunnssikkerhetsogberedskapsarbeid/?page=18

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner*.

Eggen, A. (2013). *Cybermakt - nye utfordringer i et nytt domene [FFI-Fakta]*. Kjeller.

Eide, O. K. (2017). Vi holder ikke lenge - Intervju med Sjef Cyberforsvaret, generalmajor Inge Kampenes. Hentet 15. februar 2018, fra https://forsvaretsforum.no/vår-evne-til-å-stå-i-mot-et-cyberangrep-er-marginal

Epinion Norge. (2018). *Husholdningens egenberedskap [Befolkningsundersøkelsen 2018]*. Oslo. Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/befolkningsundersokelsen2018.pdf

Etterretningstjenesten. (2017a). Digitalt grenseforsvar: Hva er det egentlig. Hentet 25. februar 2018, fra https://forsvaret.no/etjenesten/dgf

Etterretningstjenesten. (2017b). *Fokus 2017 - Etterretningstenesta si vurdering av aktuelle tryggingsutfordringar*.

Etterretningstjenesten. (2018). *Fokus 2018 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Oslo. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2018_bokmaal_oppslag_godkjent.pdf

Even, S., Siman-tov, D., & Siboni, G. (2016). Structuring Israel's Cyber Defense. *INSS Insight*, (856), 1–3. Hentet fra http://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/No. 856 - Shmulik, David, and Gabi for web.pdf

FBI, & Department of Homeland Security. (2016). *JAR-16-20296: Grizzly Steppe – Russian Malicious Cyber Activity*. u.s.

Fischerkeller, M. P., & Harknett, R. J. (2017). Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, *61*(3), 381–393. http://doi.org/10.1016/j.orbis.2017.05.003

Fishler, E. (2015). IAI to build a professional network for the cyber community in Israel. Hentet 15. april 2018, fra http://www.iai.co.il/2013/32981-46489-en/MediaRoom.aspx

FN. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly. Hentet fra http://undocs.org/A/70/174

FN. (2018a). Developments in the field of information and telecommunications in the context of international security. Hentet 14. mai 2018, fra https://www.un.org/disarmament/topics/informationsecurity/

FN. (2018b). UN ARM - Military spending. Hentet 15. mai 2018, fra http://www.un-arm.org/Milex/ReportingStatistics.aspx

Forsvarsdepartementet. (2009). *Evne til innsats - Strategisk konsept for Forsvaret*. Oslo.

Forsvarsdepartementet. (2012). *Prop. 73 S (2011–2012) Ett Forsvar for vår tid*. Oslo.

Forsvarsdepartementet. (2014). Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren. Oslo. Hentet fra https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Forsvarsdepartementet. (2016a). Kampkraft og bærekraft - Iverksettingsbrev til forsvarssektoren for langtidsperioden 2017-2020. Oslo: Forsvarsdepartementet.

Forsvarsdepartementet. (2016b). *Lov om nasjonal sikkerhet (sikkerhetsloven) (Prop. 153 L 2016 –2017)*. Hentet fra

https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf

Forsvarsdepartementet. (2016c). Prop. 151 S (2015–2016) Kampkraft og bærekraft - Langtidsplan for forsvarssektoren. Oslo.

Forsvarsdepartementet. (2017). For budsjettåret 2018 (Prop. 1 S 2017 –2018). Hentet fra https://www.regjeringen.no/no/dokumenter/prop.-1-s-fd-20172018/id2574574/sec1

Forsvarsdepartementet, & Justis- og beredskapsdepartementet. (2015). Støtte og samarbeid En beskrivelse av totalforsvaret i dag.

Forsvarsstaben. (2014). *Forsvarets fellesoperative doktrine*. Oslo: Forsvarsstaben. Hentet fra https://brage.bibsys.no/xmlui/bitstream/id/317149/FFOD 2014.pdf

Fuller, J. F. C. (1926). *The foundations of the Science of War*. (Books Express Publishing, Red.) (2002. utg.). u.s.

Geddes, B. (2003). How the approaches you choose affects the answears you get: Rational choice and its uses in comparative politics. I *Paradigms and sand castles: theory building and research design in comparative politics* (s. 175–211). Michigan: The University of Michigan Press.

Gelb, L. (2009). *Power Rules: How Common Sense Can Rescue American Foreign Policy* (Kindle). New York: Harper Collins.

Gerasimov, V. (2016). The Value of Science Is in the Foresight - Rethinking the Forms and Methods of Carrying out Combat Operations. *Military review (Oprinnelig publisert i Voyenno-Promyshlennyy Kurier 27. februar 2013. Oversatt til engelsk av Robert Coalson)*, (January-February), 23–29. Hentet fra http://www.vpk-news.ru/articles/14632

GFP. (2018). 2018 Military Strength Ranking. Hentet 25. februar 2018, fra https://www.globalfirepower.com/countries-listing.asp

Giles, K., Wirtz, J. J., Lewis, J. A., Libicki, M. C., Koval, N., Pakharenko, G., … Sakkov, S. (2015). *Cyber War in Perspective: Russian Aggression Against Ukraine*. (K. Geers, Red.). Tallinn: NATO CCD COE Publications.

Glenn, R. W. (2012). *All Glory Is Fleeting: Insights from the Second Lebanon War*. Santa Monica, CA. Hentet fra http://www.rand.org/pubs/monographs/MG708-1.html

Gloppen, K. G. (2016). *Dataavlesing i Politiets sikkerhetstjenestes forebyggende virksomhet: En rettslig analyse av om adgangen til å gjennomføre dataavlesing etter politiloven § 17 d er forenlig med retten til privatliv i Grunnloven § 102*. Universitetet i Bergen. Hentet fra https://bora.uib.no/handle/1956/15398

Gross, J. A. (2017, mai 14). Army beefs up cyber-defense unit as it gives up idea of unified cyber command. *Times of Israel*. Hentet fra http://www.timesofisrael.com/army-beefs-up-cyber-defense-unit-as-it-gives-up-idea-of-unified-cyber-command/

Gustavsen, I. H. (2015). *Når samfunnet lammes - Militær bistand ved et dataangrep*. (T. Heier & Y. Sørbye, Red.)*Militære Studier* (Bd. 2). Oslo.

Hoffman, F. G. (2007). *Conflict in the 21 st Century : The Rise of Hybrid Wars*. Arlington, VA. Hentet fra http://www.potomacinstitute.org/

Høiback, H., & Ydstebø, P. (2012). *Krigens Vitenskap*. Oslo: Abstract Forlag AS.

Hollis, D. (2011). Cyberwar Case Study: Georgia 2008. *Small Wars Journal*, (January), 1–11.

Horovitz, D. (2017, juni 22). To stop Russia and other hackers , we need to overhaul the internet, says top Israeli cyber expert. *The Times Of Israel*. Hentet fra https://www.timesofisrael.com/to-stop-russia-and-other-hackers-we-need-to-overhaul-the-internet-says-top-israeli-security-expert/

Housen-Couriel, D. (2017). *National Cyber Security Organisation: ISRAEL*. Tallinn.

IDF. (2018). Military Intelligence Directorate. Hentet 15. april 2018, fra https://www.idf.il/en/minisites/military-intelligence-directorate/

IHS Jane's. (2017). IDF setting up new Cyber Command. Hentet 14. mai 2018, fra http://www.janes.com/article/70496/idf-setting-up-new-cyber-command

Inglis, C. (2016). Cyberspace - Making some sense of it all. *Journal of Information Warfare*, *15*(2), 17–26. Hentet fra http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/stein.htm

Israel National Cyber Security Authority. (2017). Cyber defense methodology for an organization. Israel National Cyber Directorate. Hentet fra https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/en/Cyber1.0_english_617_A4.pdf

Israeldefense. (2017, mai 15). IDF Scraps Plans for a Unified Cyber Command. *IsraelDefense*. Hentet fra http://www.israeldefense.co.il/en/node/29613

Israeli Defence Forces. (2016). The IDF Strategy. u.s. Hentet fra https://www.idfblog.com/blog/2015/11/23/idf-strategy/

Israeli Government. (2011). Advancing National Cyberspace Capabilities: Resolution No. 3611 of the Government of August 7, 2011 (Non-official). Hentet 18. september 2017, fra http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/D

ocuments/Advancing National Cyberspace Capabilities.pdf

Israeli National Cyber Bureau. (2015). Background for the Government Resolutions Regarding Advancing the National Preparedness for Cyber Security and Advancing National Regulation and Governmental Leadership in Cyber Security. u.s.: State of Israel - Prime Minister's Office. Hentet fra https://ccdcoe.org/sites/default/files/documents/Background_for_the_Government_Resolutions_Regarding_Cyber_Security-February_2015.pdf

Jervis, R. (2016). Some Thoughts On Deterrence In The Cyber Era. *Journal of Information Warfare, 15*(2).

Johnsen, S. T. (2014). *Norway, NATO and cyber defense - FFI-rapport 2014/01328*. Kjeller.

Justis- og beredskapsdepartementet. (2012). Samfunnssikkerhet. (Meld.St nr. 29, 2011-2012). Hentet fra https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/

Justis- og beredskapsdepartementet. (2017). Meld. St. 38 (2016-2017) IKT-sikkerhet: Et felles ansvar.

Kantar TNS. (2017). *Forsvarets innbyggerundersøkelse*. Oslo. Hentet fra https://forsvaret.no/fakta_/ForsvaretDocuments/Innbyggerundersokelsen 2017.pdf

Kommunal- og moderniseringsdepartementet. (2015). Handlingsplan for informasjonssikkerhet i statsforvaltningen – 2015–2017. Oslo: Kommunal- og moderniseringsdepartementet Offentlige. Hentet fra https://www.regjeringen.no/contentassets/b7d0918e555b418abda2993a71969cdc/handlingsplan_informasjonssikkerhet_staten.pdf

Kuehl, D. T. (2009). Cyberspace and cyberpower. I F. D. Kramer, S. H. Starr, & L. K. Wentz (Red.), *Cyberpower and national security*. Washington, DC: National Defense University Press.

Langø, H. (2013). Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security. Oslo: NUPI (NIIA).

Lapid, E., & Gilboa, A. (2012). *Israel's Silent Defender: An inside Look at Sixty Years of Israeli Intelligence* (Kindle). Jerusalem: Gefen Publishing House Ltd.

Leshem, M. (1998). *Israel's National Security Strategy: Past and Future Perspectives*. Carlisle, PA. Hentet fra http://www.dtic.mil/dtic/tr/fulltext/u2/a346921.pdf

Libicki, M. C. (2016). *Cyberspace in Peace and War*. Annapolis, MD: Naval Institute Press.

Løvold, A. (2004). Småstatsproblematikken i internasjonal politikk. *Internasjonal Politikk, 62*(1), 7–31.

Lysne, O., Grytting, T., Jarbekk, E., Lunde, E., & Reusch, C. (2016). *Digitalt grenseforsvar (DGF)*. Oslo.

Magid, J. (2017, april 24). Security chiefs slam Netanyahu over planned cyber defense body. *Times of Israel*. Hentet fra https://www.timesofisrael.com/security-chiefs-slam-netanyahu-over-planned-cyber-defense-body/

Matthews, M. (2008). *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*. *The Long War Series Occasional Paper*. Kansas. Hentet fra papers2://publication/uuid/5B051E57-6A88-4BC3-81BF-BBC50BBD4A62

Minister for Law Enforcement and Cyber Security. (2018). Australian Government attribution of the 'NotPetya' cyber incident to Russia. Hentet 15. mai 2018, fra http://minister.homeaffairs.gov.au/angustaylor/Pages/notpetya-russia.aspx

Mørkestøl, K. H. (2014). Cyber: Buzzword or Game Changer? How the Digital Space Affects National and International Security. I R. Allers, C. Masala, & R. Tamnes (Red.), *Common or Divided Security? German and Norwegian Perspectives on Euro-Atlantic Security*. (s. 85–103). Frankfurt: Peter Lang Edition.

Mossad. (2017). Libertad Tehcnological innovation fund. Hentet 27. april 2018, fra http://www.libertad.gov.il/eng/index.html

Muller, L. P. (2016). Makt og avmakt i cyberspace: hvordan styre det digitale rom? *Internasjonal politikk*, *74*(4), 1–23. http://doi.org/https://doi.org/10.17585/intpol.v74.428

Muller, L. P. (2017). Upholding the NATO cyber pledge Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics. Hentet 15. mai 2018, fra http://www.nupi.no/Publikasjoner/CRIStin-Pub/Upholding-the-NATO-cyber-pledge-Cyber-Deterrence-and-Resilience-Dilemmas-in-NATO-defence-and-security-politics

Nasjonal Sikkerhetsmyndighet. (2017). Rammeverk for håndtering av IKT-sikkerhetshendelser. Oslo. Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

NATO. (2016a). *AJP-2.1 Allied Joint Doctrine for Intelligence Procedures* (Edition B). u.s.: NATO Standardization office (NSO).

NATO. (2016b). Cyber Defence Pledge. Hentet 13. september 2017, fra http://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2016c). Warsaw Summit Communiqué. Hentet 13. september 2017, fra http://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO Cooperative Cyber Defence Centre of Excellence. (2018). Cyber definitions. Hentet 2. april 2018, fra https://ccdcoe.org/cyber-definitions.html

NATO Standardization Agency. (2016). AAP-6: NATO Glossary of Terms and Definitions (English and French).

Netanyahu, B. (2016). PM Netanyahu's Full Remarks at CyberTech 2016 [Videoklipp]. Hentet fra https://www.youtube.com/watch?v=KqKfanu1e5w

Netanyahu, B. (2017). PM Netanyahu's Remarks at CyberTech 2017 [Videoklipp]. Hentet fra https://www.youtube.com/watch?v=4x2v0VwgxPc

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo.

NOU 2016:19. (2016). *Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Oslo: Departementenenes servicesenter.

NSM. (2014). Varslingssystem for digital infrastruktur (VDI). Hentet 31. mars 2018, fra https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/

Opall-Rome, B. (2017, oktober 9). Massive drill validates Israel's cyber-secure C4I network. Hentet 28. april 2018, fra https://www.c4isrnet.com/it-networks/2017/10/09/massive-drill-validates-israels-cyber-secure-c4i-network/?utm_source=Sailthru&utm_medium=email&utm_campaign=PT Daily Brief 10.10.17&utm_term=Editorial - Daily Brief

Paikowsky, D., & Ben Israel, I. (2009). Science and technology for national development: The case of Israel's space program. *Acta Astronautica*, *65*(9–10), 1462–1470. http://doi.org/10.1016/j.actaastro.2009.03.073

Paret, P., Craig, G. A., & Gilbert, F. (1986). *Makers of Modern Strategy: From Machiavelli to the Nuclear Age*. (P. Paret, Red.). New Jersey: Princeton University Press.

Parker, G., Hanson, V. D., Bachrach, B. S., Allmand, C., Seed, P., Lynn, J. A., & Murray, W. A. (2009). *The Cambridge history of warfare*. (G. Parker, Red.) (2. utg.). New York: Cambridge University Press.

Politidirektoratet. (2014). Etterretnings-doktrine for politiet. Politidirektoratet.

Politidirektoratet. (2015). *Overordnet nasjonal strategi for bekjempelse av datakriminalitet - Datakrimstrategien*.

Politidirektoratet. (2017). *Trusler og utfordringer innen IKT-kriminalitet*. Oslo.

Politiet. (2018). Kripos. Hentet 15. mai 2018, fra https://www.politiet.no/om/organisasjonen/sarorganene/kripos/

Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf

Politiloven. (1995). Lov om politiet m.v. av 01.10 1995. Hentet fra https://lovdata.no/dokument/NL/lov/1995-08-04-53

Porche III, I. R., Paul, C., Serena, C. C., Clarke, C. P., Johnson, E., & Herrick, D. (2017). *Tactical Cyber - Building a Strategy for Cyber Support to Corps and Below*.

Ravndal, Ø. (2016). *Øket Russisk Operativ Evne – Implikasjoner for Norges evne til å Avverge eller Motstå et Væpnet Angrep*. Forsvarets høgskole.

Regjeringen. (2017a). UN Res 71/28 "Developments in the field of information and telecommunications in the context of international security". Hentet 14. mai 2018, fra https://s3.amazonaws.com/unoda-web/wp-content/uploads/2017/09/Norway.pdf

Regjeringen. (2017b). Utreder et digitalt grenseforsvar. Hentet 15. mai 2018, fra https://www.regjeringen.no/no/aktuelt/utreder-et-digitalt-grenseforsvar/id2539809/

Regjeringen. (2018). Framtidige anskaffelser til forsvarssektoren 2018-2025 (FAF 2018-2025). Hentet 15. mai 2017, fra https://www.regjeringen.no/no/aktuelt/framtidige-anskaffelser-til-forsvarssektoren-2018-2025-faf-2018-2025/id2593750/

Regjeringen Bondevik II. (2003). Nasjonal strategi for informasjonssikkerhet - Pressemelding 08.07.2003. Hentet 4. januar 2018, fra https://www.regjeringen.no/no/aktuelt/nasjonal_strategi_for_informasjonssikker/id249670/

Ricks, T. E. (2017, desember 7). NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons. *Foreign Policy*. Hentet fra http://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. http://doi.org/10.1080/01402390.2011.608939

Rid, T. (2013). *Cyber War Will Not Take Place*. New York: Oxford University Press.

Rid, T. (2016). *Rise of the machines: A cybernetic history [Kindle]*. New York: W. W. Norton & Company.

Ringdal, K. (2013). *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode* (3. utg.). Bergen: Fagbokforlaget.

Rivera, J. (2015). Achieving cyberdeterrence and the ability of small states to hold large states

at risk. I M. Maybaum, A.-M. Osula, & L. Lindström (Red.), *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. Tallinn: NATO CCD COE Publications. http://doi.org/10.1109/CYCON.2015.7158465

Rosenberg, S. (2016). *Deterring Terror: How Israel Confronts the Next Genration of Threats - English Translation of the Official Strategy of the Israel Defence Forces*. Cambridge.

Samfunnssikkerhetsinstruksen. (2017). Instruks for departementenes arbeid med samfunnssikkerhet m.v. av 01.09.2017. Hentet fra https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349

Shlaim, A. (2014). *The Iron Wall: Israel and the arab world [Kindle]* (2. utg.). New York: W. W. Norton & Company. Hentet fra https://read.amazon.com/?asin=B00O950HLY

Sikkerhetsloven. (1998). Lov om forebyggende sikkerhetstjeneste m.v. av 01.07 2001. Hentet fra https://lovdata.no/dokument/NL/lov/1998-03-20-10

Silverstein, R. (2016). Mossad Launches Cyber-war Unit with Neewspaper Want Ads [blogg post]. Hentet 27. april 2018, fra https://www.richardsilverstein.com/2016/05/11/mossad-launches-cyber-war-unit/

Singer, P. W., & Friedmann, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press.

Statsministerens kontor. (2013). Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet. Hentet fra https://lovdata.no/dokument/DEL/forskrift/2013-03-22-296

Sterling-Folker, J. (2010). Neoliberalism. I *International Relations Theories Disipline and Diversity* (s. 114–131). Oxford: Oxford University Press.

Storruste, B., Magnussen, T., Børset, B., Aga, A. C. I., Thorkildsen, S. E., Austad, T., … Hansen, E. T. (2012). *Politiet i det digitale samfunnet*. Oslo.

Straffeprosessloven. (1981). Lov om rettergangsmåten i straffesaker m.v. av 01.01 1986. Fjerde del. Tvangsmidler. Kap 16 d. Dataavlesing. Hentet fra https://lovdata.no/dokument/NL/lov/1981-05-22-25/KAPITTEL_4-10#KAPITTEL_4-10

Tabansky, L. (2013). Critical Infrastructure Protection Policy: The Israeli Experience. *Journal of Information Warfare*, *12*(3), 78–86.

Tabansky, L. (2016a). Cyber Power in the changing Middle East. *Turkish Policy Quarterly*, *15*(1), 107–114. Hentet fra http://turkishpolicy.com/files/articlepdf/cyber-power-in-the-changing-middle-east_en_2071.pdf

Tabansky, L. (2016b). Towards a Theory of Cyber Power: The Israeli Experience with Innovation and Strategy. I N. Pissanidis, H. Rõigas, & M. Veenendaal (Red.), *2016 8th International Conference on Cyber Conflict* (s. 51–63). Tallinn: NATO CCD COE Publications. Hentet fra https://ccdcoe.org/cycon/2016/proceedings/04_tabansky.pdf

Tabansky, L., & Ben-Israel, I. (2015). *Cybersecurity in Israel*. u.s.: Springer eBooks. Hentet fra https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo_library/libweb/action/search.do?fn=search&ct=search&initialSearch=true&mode=Basic&tab=default_tab&indx=1&dum=true&srt=rank&vid=FHS&frbg=&tb=t&vl%2528freeText0%2529=cybersecurity+in+israel&scp.scps=scope%25

Trædal, T. J. (2017, november 16). Nå får politiet sitt «NC3» - et eget senter for cyberkriminalitet. *Politiforum*. Hentet fra https://www.politiforum.no/artikler/na-far-politiet-sitt-nc3-et-eget-senter-for-cyberkriminalitet/412189

US Army. (2017). *FM 3-12 Cyberspace and Electronic Warfare Operations*. Washington D.C.

Utenriksdepartementet. (2017). Internasjonal cyberstrategi for Norge 2017. Oslo.

van Niekerk, B., & Maharaj, M. (2009). The Future Roles of Electronic Warfare in the Information Warfare Spectrum. *Journal of Information Warfare*, *8*(3), 1–13.

Ward, C. (2007, november 26). Israel's Cyber Shot at Syria. Hentet 18. september 2017, fra https://www.defensetech.org/2007/11/26/israels-cyber-shot-at-syria/

Yadin, Y. (1991). For by wise counsel thou shalt make thy war: A strategical analysis of last year's battles [Condensed translation of article published in Bamachaneh (The Israel Forces' Journal), September 1949]. I B. H. Liddell Hart (Red.), *Strategy (Rev. utg. av: Decisive wars in history. London. G. Bell & Sons, 1929. - Reprint av tidl utg. New York: Praeger, 1967)* (2. rev. ed, s. 386–405). New York: Meridian.

Yanai, N. (1989). BEN-GURION'S CONCEPT OF MAMLAHTIUT AND THE FORMING REALITY OF THE STATE OF ISRAEL. *Jewish Political Studies Review*, *1*(1–2 (Spring)), 151–177. Hentet fra http://jcpa.org/wp-content/uploads/2012/11/bengurions-concept.pdf

Yin, J. K. H. (2009). The Electronic Intifada: The Palestinian Online Resistance in the 2nd Intifada. *Journal of Information Warfare*, *8*(1), 1–19.