Necesse 2018, Vol 3, Issue 2, 108-122 DOI: 10.21339/2464-353x.3.2.108

Lederskap, makt og cyber

Øyvind Jøsok[1,2]

[1] Forsvarets Høgskole, Forsvarets Ingeniørhøgskole, Lillehammer
[2] Høgskolen i Innlandet, Lillehammer
ojosok@cyfor.mil.no, ojosok@inn.no

Sammendrag. Militære operasjoner beskrives som stadig mer komplekse. I denne teksten drøftes cyberdomenet som drivkraft for denne utviklingen. Det argumenteres for at cyberdomenet har betydning for organisering av stridskreftene innen de tradisjonelle krigføringsdomenene i Norge; land, luft og sjø. Videre belyses det hvordan cyberdomenet griper inn i, og utfordrer, rådende forestillinger om maktstrukturer i Forsvaret, og i samfunnet ellers. Til slutt argumenteres det for at cyberdomenets økende betydning påvirker hvordan ledelse i Forsvaret utøves. Sentralt i argumentasjonsrekken står Forsvarets erfaringer fra satsning på nettverksbasert forsvar, Moses Náims bok; "The end of power" og General Stanley McChrystals bok; "Teams of teams". Kildene forenes i denne argumentasjoner gjennom fellestrekket hierarkisk tenkning i en nettverksbasert realitet.

Nøkkelord: Lederskap, Makt, Cyberdomenet, Cybermakt, Forsvaret

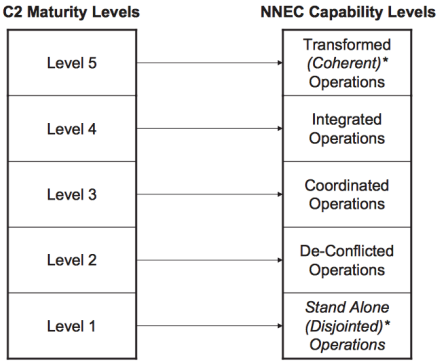
1 Hierarki og nettverk

1.1 Introduksjon

Det har lenge vært akseptert at det finnes like mange definisjoner av ledelse som det finnes mennesker som har prøvd å definere begrepet (Strand, 2007). Makt på sin side har i det egalitære Norge en noe negativ ladning (i motsetning til det engelske synonymet "power"), og dermed ofte tabu i samme setning som lederskap. Cyberdomenet på sin side er også et begrep som det hersker usikkerhet rundt betydningen av, og i hvilken grad det vil være et viktig element av fremtidige militære operasjoner (Lund, 2017). Muliggjør cyberdomenet militære operasjoner, eller er det et eget domene for militære operasjoner? Er cybermakt en realitet? Og har da cyberdomenet betydning for utøvelse av lederskap? I denne teksten vil de tre begrepene; lederskap, makt og cyberdomenet bli brukt i argumentasjonen, selv om det eksisterer svakheter i betydningen av det enkelte begrep. Argumentasjonen forsøker å rette fokus på hvordan disse begrepene påvirker hverandre, og hva de til sammen har å bety for utøvelse av ledelse i Forsvaret - nå og inn i fremtiden. Mer presist så vil følgende problemstilling bli drøftet: Hvordan påvirker cyberdomenet utøvelsen av lederskap i Forsvaret?

1.2 Nettverksbasering

Nettverksbasert Forsvar (NbF) har det siste tiåret vært et av de store satsningsområdene til det NATO. Allerede i 2002 ble de enighet i NATO C3 Board om å utvikle et NATO konsept som forente de ulike nettverksbaseringsinitiativene som fantes i alliansen (NC3A, 2005), og i 2010 ble NATO Network Enabled Capability (NEC) Command and Control Maturity Model utviklet (ACT, 2010). Denne modellen (Figur 1) beskriver fem nivå med tilhørende mål for graden av nettverksbasering, der nivå én er adskilte operasjoner, og nivå fem er fullintegrerte og nettverksbaserte operasjoner. Fundamentet for nettverksbasering er innføring av avansert nettverksteknologi.



Figur 1: NATO NEC Maturity Levels (ACT, 2010)

På Norsk side omtaler Forsvarets fellesoperative doktrine fra 2007 'evne til å operere i nettverk' og 'nettverksbasering' eksplisitt, og teknologiutviklingen innen informasjons- og ledelsessystem fremheves som en viktig driver for utviklingen (FFOD, 2007). Doktrinene fremhever nettverkstenking, sammen med effekttenking og manøvertenking, som det idémessige grunnlaget i militære operasjoner (FFOD, 2007). Videre defineres nettverkstenking som; "... å organisere sine ressurser mest mulig effektivt for å oppnå størst mulig systemintegrasjon, situasjonsbevissthet og forståelse av sjefens intensjon, og omfatter utvikling av mennesker, organisasjon og teknologi." (FFOD, 2007, s. 173). Etter modell fra NATO har først Sjef INI og deretter Sjef Cyberforsvaret vært ansvarlig for nettverksbaseringen av Forsvaret. FFOD (2007) setter også ambisjonsnivået for graden av nettverksbasert forsvar tydelig på agendaen:"Innledende NbF vil være innenfor rekkevidde i løpet av noen år. Et forsvar i denne fasen vil ha en organisasjon med gjennomgående gode kunnskaper om NbF, og NbF vil være en integrert del av all utdanning og trening." (FFOD, 2007, s. 97). I en evaluering av FFIs støtte til implementeringsprosessen konkluderes det med at det er vanskelig å si om fokuset på nettverksbasering av Forsvaret har gitt noen operativ effekt, eller om det bare har vært en naturlig forbedringsprosess (FFI, 2016). Det som forøvrig er interessant i konteksten 'cyberdomenets betydning for lederskap', er at rapporten fatter stor interesse for en vesentlig faktor; Nettverksbasering handler om å organisere i nettverk. Forsvaret er en sterkt hierarkisk organisasjon. Mennesker ser ut til å være flaskehalsen i denne spenningen, uten at det har vært gjort gode nok grep for å håndtere utfordringen under utdanning og trening av personell (FFI, 2016).

"Hvis militært personell er ment å tenke og handle i nettverk, så må de trenes og utdannes til dette. I dag tar all grunnleggende militær trening og tenkning utgangspunkt i hierarkier. Hierarkier er en grunnleggende annerledes måte å organisere arbeid på enn nettverk. For å bedre samhandling og kommunikasjonsflyt i Forsvaret, må menneskene i organisasjonen samhandle og kommunisere bedre og på andre måter enn det som er tilfellet i dag. Etter mange tiår med stor teknologioptimisme er det nødvendig å diskutere hvordan de mellommenneskelige utfordringene som er identifisert og definert kan endres, bedres og håndteres. I en militær kontekst er det nærliggende å peke på seleksjon, trening, utdanning og godt, gammeldags lederskap." (FFI, 2016, s. 33).

FFI (2016) peker her på et gap mellom visjonen nettverksbasert Forsvar og realiteten som preger organisasjonen.

1.3 Visjonen

Fra politisk nivå er det en tydelig uttalt ambisjon å satse på et høyteknologisk Forsvar (Se f.eks: (Prop. 151 Stortingsproposisjon, 2016); (Meld. St. Stortingsmelding, 2013)). Store materiellinvesteringer i alle grener (eks. F-35, Fregatt, oppgradering av CV90) vitner om evne og vilje til å investere i ny teknologi for å realisere visjonen. Utfordringen som bare vagt adresseres i FFOD fra 2007, og i liten grad i FFOD fra 2014, er at ved å investere i høyteknologiske plattformer og knytte disse sammen i nettverk, har man etablert en nytt domene på tvers av de eksisterende domenene; cyberdomenet. Cyberdomenet som operasjonsdomene er i seg selv interessant (Lund, 2017) men denne teksten vil ta for seg cyberdomenets påvirkning på andre deler av Forsvarets virke. FFI (2016)peker i sin rapport på mellommenneskelige utfordringer, Johnsen (2013) mener cyberdomenet utfordrer tradisjonelle forestillinger om organisering, FFOD (2014) påpeker at utviklingen utfordrer etablerte måter å lede på og Naím (2013) argumenterer for at den tradisjonelle forestillingen om makt endres. For å kunne besvare problemstillingen vil den videre teksten analysere de tre faktorene cyberdomenet, makt og lederskap med hensyn på spenningsfeltet mellom hierarki og nettverk.

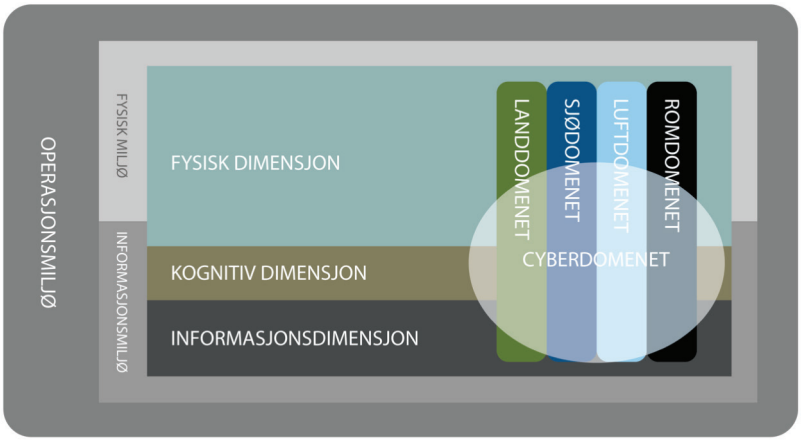
2 Cyberdomenet

2.1 En definisjon?

Bruken av prefikset cyber er ifølge Lund (2017) langt fra konsistent. Det fører til uklarheter når vi skal forholde oss til cyberdomenet som et domene for krigføring (Lund, 2017). Det finnes i dag en mengde definisjoner og begreper i den norske interessesfæren der enten cyberdomenet, eller lignende begreper for å beskrive det samme fenomenet, benyttes. NATO Cooperative Cyber Defence Centre of Excellence henviser til den Finske definisjonen av cyberdomenet (NATO, 2017). Den Finske versjonen er å finne i den Finske "Cyber Security Strategy" fra 2014 (MoD, 2013). Her defineres cyber-

domenet som: ”Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures”. I FFOD (2014) omtales cyberdimensjonen, det datamaskingenererte rom og det digitale rom synonymt. Samme år omtaler Forsvarsdepartementet cyberdomenet i sine cyberretningslinjer (FD, 2014). Her defineres cyberdomenet som; ”Fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data.” (FD, 2014, s. 4). Likheten mellom definisjonene som refereres til er at de belyser de teknologiske aspektene ved cyberdomenet. Spørsmålet som da gjenstår å besvare er om cyberdomenet bare er et menneskeskapt teknologisk domene, eller om det er noe mer. Lund (2017) trekker frem følgende betraktning: ”Cyberdomenet er en artefakt forma av intensjonane til skaparane, eigarane og brukarane av nettverk, system, maskinvare og programvare.” (Lund, 2017, s. 30). Dette er et perspektiv som belyser det faktum at en egenskap ved cyberdomenet er at det kan utnyttes på måter som domenet ikke er skapt for, eller intendert for (Lund, 2017). Noe som indikerer at cyberdomenet har egenskapen til å, direkte eller indirekte, påvirke andre domener og dimensjoner (Brangetto & Veenendaal, 2016).

Figur 2 er hentet fra NATOs pågående arbeid med å utarbeide en doktrine for cyberoperasjoner (AJP_3-20, Draft). Her spenner cyberdomenet over de fire tradisjonelle domenene - land, sjø, luft og verdensrommet. I tillegg spenner cyberdomenet over den fysiske dimensjonen, den kognitive dimensjon og informasjonsdimensjonen. Figuren viser at cyberdomenet kan påvirke både den fysiske sfæren til militære beslutningstagere, måten de forstår verden på, og den informasjon og kunnskap de er avhengig av for å kunne operere. I og gjennom cyberdomenet kan man altså i teorien påvirke og ramme både landoperasjoner, luftoperasjoner, sjøoperasjoner og operasjoner i verdensrommet på tvers av de tre dimensjonene. Et ganske altomfattende perspektiv. Samtidig illustrerer figuren at cyberdomenet i seg selv har fysiske, kognitive og informasjon attributter, i likhet med andre militære domener.



Figur 2: Gjengitt etter skisse i NATO AJP 3-20 (AJP_3-20, Draft)

Mangfoldet av definisjonen og begreper som brukes til å beskrive fenomenet som i denne teksten omtales som cyberdomenet er stort, noe som tyder på at den kognitive dimensjonen av cyberdomenet, altså forståelsen av domenet, er mangelfull. Selve cyberdomenet ser ut til å være i militær sammenheng noe prematurt og lite utviklet (Lund, 2017), iallfall i det Norske Forsvaret. Videre tyder det på at den fysiske dimensjonen av cyberdomenet fortsatt er underutviklet, siden Forsvaret ikke har nådd målene innen nettverksbasering med full sømløs integrasjon av alle plattformer, og dertil effektiv utveksling av informasjon for å understøtte beslutningstagere som skissert i FFOD (2014).

Figur 2 kan kanskje også illustrerer hvorfor cyberdomenet er et omdiskutert tema i militær sammenheng. I denne figuren fremstilles cyberdomenet foran og på tvers av de eksisterende krigføringsdomener. Denne fremstillingen utfordrer eksisterende tenkning og forståelse av militære operasjoner, og ikke minst etablerte hierarki og maktstrukturer innad i domenene. Selv om dette påpekes i FFOD (2014) som en konsekvens av nettverksbasering, er Forsvaret i økende grad tvunget til å ta innover seg at man må forholde seg til cyberdomenet på andre måter enn som muliggjører for samband mellom avdelinger og muliggjører for kommando og kontroll av militære enheter. Nettverksbasering har ført til etablering av cyberdomenet som i seg selv er et krigføringsdomene der makt kan utøves, eller projiseres gjennom (Haaster, 2016). Den part med best evne til å utnytte disse fordelene ved cyberdomenet vil kunne få store operasjonelle fordeler i militære operasjoner (Johnsen, 2013).

2.2 Cybermakt

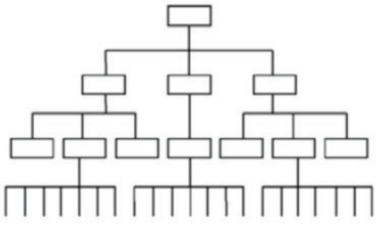
Innføring av luftmakt endret rollen til land og sjøstyrkene (Aron, 1955). Men selv om luftmakten var en realitet tidlig på 1900-tallet, var det i lang tid etterpå vanskelig å konseptualisere og konkretisere hva luftmakt egentlig var. Et sitat fra Winston Churchill i etterkant av andre verdenskrig illustrerer dette godt: "Air power is the most difficult of all forms of military force to measure or even to express in precise terms" Winston Churchill, 1948 (I Allen & Machain, 2017, s. 1). I 2017 ser det ut til at utviklingen av cybermakt følger en lignende bane. Erkjennelsen av cyberdomenet som krigføringsområde (NATO, 2016) og domenets potensiale som våpen (Johnsen, 2013), påvirker også rollen til de andre domenene. Selv om cyberdomenet har vært en realitet lenge, så er det fortsatt vanskelig å konseptualisere og konkretisere akkurat hva denne endringen er (Lund, 2017). Spørsmålet er fortsatt i hvilken grad, og hvilket omfang av endring, utviklingen av cybermakt vil utgjøre for de andre krigføringsområdene.

Cyberdomenet preges av både fysiske og ikke fysiske artefakter (Lund, 2017). Cyberdomenet knytter de ulike domenene sammen og muliggjør multi-domene operasjoner (Perkins, 2017). Samtidig visker cyberdomenet ut grensene mellom domener og dimensjoner i den forstand at det blir vanskeligere å skille mellom "cause and effect". Dette beskrives som mer kompleksitet i operasjonsmiljøet (McChrystal, Collins, Silverman, & Fussell, 2016). Dette fører til flere avhengigheter som må tas hensyn til, og det blir mer krevende å ha oversikt over alt som skjer innenfor domener og dimensjoner (Buchler et al., 2016). Disse egenskapene ved cyberdomenet gjør cyberdomenet egnet til, for en kapabel motstander, å påvirke andre domener i og gjennom den fysiske-

, kognitive- og informasjon dimensjonen som vist til i figur 2. Cybermakt er derfor ikke en triviell sak å definere på nåværende tidspunkt. De tilgjengelige definisjonene bærer preg av å inkludere alt. På den ene siden kan dette virke riktig med henvising til figur 2, men på den andre siden illustrerer dette også en slags avmakt i definisjonsprosessen der det fremstår usikkert hva cybermakt *egentlig* er, og hvilket omfang cybermakt har. I den videre drøftingen støtter denne teksten seg på følgende forståelse av cybermakt: *"Cyber power comprises the variety of powers affecting the geographic, physical network, logical, and cyber persona components, which consequently shape the experiences of state and non-state actors who act in and through cyberspace."* (Haaster, 2016, s. 14). Med henvisning til figur 2 kan cybermakt da forstås som å påvirke andre domener gjennom å utnytte den fysiske dimensjonen (f.eks ved å fysisk ta kontroll over nettverk), informasjonsdimensjonen (f.eks ved å bruke cyberangrep til å manipulere informasjon) eller den kognitive dimisjonen (f.eks ved å bruke sosiale media profiler til å påvirke) av cyberdomenet. Med denne forståelsen må cyberdomenet og cybermakt behandles som noe mer enn nettverksteknologi og cyberangrep.

2.3 Den menneskelige faktor

Innføring av nettverksbasert Forsvar, og dermed etablering av cyberdomenet, har handlet om teknologi (Andreassen, 2017). Det har handlet om å omstille et lavteknologisk invasjonsforsvar til et høyteknologisk innsatsforsvar. Men nettverksbaseringen har hatt begrenset effekt (FFI, 2016). I likhet med FFI påpeker Andreassen (2017) svakheter ved utdanning, trening og øving i forbindelse med nettverksbasering av Forsvaret. Det er indikasjoner på at det har vært og er klare skiller mellom innføring av teknologi, utdanning innen bruk av teknologi og det å lede i et nettverksbasert Forsvar, noe som fører til redusert og forsinket evne til å utnytte teknologi (Andreassen, 2017). Det har ikke vært tilstrekkelig investert i menneskene og konkret påpekes det svakheter innenfor samhandling og kommunikasjon (FFI, 2016). Noe som har ført til en forsinket evne til å ta i bruk ny teknologi. *"The delayed implementation of Network Based Defence affects the entire Norwegian Armed Forces and puts military lives and operations at stake"* (Andreassen, 2017, s. 19). Hva er det som gjør at samhandling og kommunikasjon reduserer effekten av NbF-satsningen? En grunn kan være at all grunnleggende militær utdanning i Forsvaret i dag tar utgangspunkt i hierarkier, og at dette er en grunnleggende annerledes måte å tenke på enn nettverk (FFI, 2016). En hypotese er altså at Forsvaret har prøvd å innføre nettverkstenking uten å endre måten vi tenker på.



Figur 3: Hierarki og nettverk (FFI, 2016)

Alle de tradisjonelle domenene i det Norske Forsvaret er organisert i hierarki. Cyberdomenet muliggjør fysisk og logisk sammenkobling i nettverk (Figur 3). Slik skapes nettverk, og nettverk av nettverk, innad i og mellom tradisjonelle strukturer. I tillegg til de formelle nettverkene, Forsvarets egne systemer, eksisterer også uformelle nettverk (F.eks bruk av mobiltelefon, sosiale media etc.) som skapes og utnyttes av Forsvarets personell for å løse oppdrag. Disse uformelle nettverkene har fått stadig større betydning og aksept som en normal del av militære operasjoner (trening, øving og skarpe oppdrag). Samtidig blir Forsvaret stadig mer avhengig av sivil nettverksinfrastruktur og sivile leverandører og underleverandører som utelukkende utnytter sivil nettverksinfrastruktur. Dette er et resultat av egenskapene til cyberdomenet. Cyberdomenet muliggjør sammenkobling og informasjonsutveksling, noe som er nyttig for kommando og kontroll, men det skaper samtidig utfordringer i den menneskelige dimensjonen både hva gjelder makt og lederskap. Noe som er tema i de to neste delene av teksten.

3 Makt

3.1 Makt i endring

"Power is the ability to direct or prevent the current or future actions of other groups or individuals. Or, put differently, power is what we exercise over others that leads them to behave in ways they would not otherwise have behaved" (Naím, 2013)

Moisés Naím (2013) argumenterer i sin bok "The end of power" for at makt gjennomgår en transformasjon der sentraliserte hierarkiske mastodonter taper makt til fordel for mindre uorganisert grupper eller individer. Han baserer sin argumentasjon på tre faktorer; 'more', 'mobility' og 'mentality'. Den første faktoren, more, innebærer det faktum at det i dag finnes mer av alt. Når det finnes flere mennesker, og disse har muligheten til å leve et mer tilfredsstillende liv, er konsekvensen at de blir vanskeligere å kontrollere. Individer kan i større grad være mobile fordi det er billigere, raskere og enklere å gjøre. Resultatet er at individ mikses sammen på tvers av kultur, religion og andre demografiske skillelinjer. De to forestående faktorene har resultert i at mennesker raskere endrer mentalitet. Mer kunnskap og kompetanse betyr at den enkelte krever mer og forventer mer av maktstrukturene som regjerer, på alle nivå (Naím, 2013). Naím attribuerer ikke denne endringen i makt til cyberdomenet alene, men argumentert for at cyberdomenet i økende grad er en arena for påvirkning og utøvelse av makt. Derfor er det interessant å se nærmere på hvordan makt og cyberdomenet påvirker hverandre i en militær kontekst.

Grunnleggende i utøvelsen av makt er at maktstrukturen må ha kapasitet til å kunne utøve denne makten. Det vil si evne og vilje. I militære strukturer har dette vært synonymt med kommando og kontroll. En formell tilgang på makt gjennom kapasitet (soldater og våpen) og formalitet (posisjon), og evne til å kontrollere utøvelsen av denne

(Forsvaret, 2012). Tradisjonelt har mer makt vært bedre enn mindre makt, og måleenheten har vært mengde og teknologi. Denne forståelse av makt er ifølge Naím (2013) i ferd med å endre seg radikalt. Han argumenterer for at endringene som følge av more, mobility og mentality favoriserer 'micropowers' og er i 'megaplayers' disfavør. Megaplayers er i denne sammenheng å betrakte som en nasjons eller koallisjons militærmakt, og micropowers små grupper eller individer som har evne og vilje til å nekte megaplayers å seire i en konflikt (Naím, 2013). Eksemplene på nettopp dette begynner det å bli mange av. Men likevel er den rådende oppfatningen at en teknologisk avansert militærmakt er essensielt for en nasjons sikkerhet (Naím, 2013), spørsmålet er om denne karakteristikken av makt er dekkende i den moderne konteksten: "Today, national armies are attempting to adjust - with different speeds and results - to "full spectrum" warfare in which weapons are digital as much as physical methods are psychological as much as coercive, and combatants are civilian and scattered as much as uniformed and coordinated" (Naím, 2013, s. 123).

3.2 Lende og tid

En av karakteristikkene som har endret seg er at konflikter i mindre grad er knyttet til fysisk territorium (Naím, 2013). Noe som også i høyeste grad er gjeldende for cyberdomenet og utøvelsen av cybermakt."Cyberpower gives the little guys the kind of ability that used to be confined to superpowers" (Amos Yadlin, 2009 i Naím, 2013). Dette er forøvrig ingen ny tanke, siden enhver militærteoretiker vil påstå at konflikter vinnes og tapes i det kognitive domenet[1] (FFOD, 2007). Cybermakt vil derfor kunne dele egenskaper med andre domeners forståelse av makt, forskjellen er derimot at 'lendet' er av en annen karakteristikk (Bibighaus, 2015). Her kan det argumenteres for at selve lendet er formbart i en større grad enn i de andre domenene, siden lendet (cyberdomenet) i seg selv er menneskeskapt (Lund, 2017). Det vil implisitt si at dersom man ikke har etablert cyberdomenet innad i f.eks en nasjon, vil det være umulig for en motstander å utøve cybermakt i og gjennom cyberdomenet for å påvirke opinionen. Noe som kan argumenters for er situasjonen i Nord-Korea, digitalisering av landet på et så lavt nivå at cyberdomenet ikke eksisterer (Naughton, 2017).

En annen karakteristikk som har endret seg, er tid, i dobbel forstand. Cyberdomenet er gjennom teknologisk utvikling alltid gjenstand for endring, rask endring. Som General Amos Yadlin påpeker; "Staying ahead of the game is important in light of the dizzying change of pace in the cyber-world, at most, a few months in response to a change, compared to the years pilots had" (Amos Yadlin, 2009 i Naím, 2013) Samtidig blir langsiktige initiativ med mål om å plante bakdører eller tilganger til systemer og nettverk for fremtidig bruk vanligere (F.eks Operation Nitro Zeus[2]). Konsekvensen blir

[1] Forsvarets Fellesoperative Doktrine (FFOD) bruker begrepet det kognitive domenet. Tidligere har det vært referert til den kognitive dimensjonen. Disse begrepene behandles som synonymer i denne teksten og har samme betydning.

[2] Operation Nitro Zeus er ikke bekreftet av offisielle kilder, men skal være i følge dokumentaren Zero Days (Gibney, 2016) være et initiativ fra amerikanske National Security Agency (NSA) med mål om å infiltrere Iranske våpen og datasystem i tilfelle eskalering av konflikten i kjølevannet av STUXNET angrepet.

at en motstander som har god tid, og evner å iverksette langsiktige initiativ, gjerne i årevis eller mer, er bedre til å utnytte cyberdomenet enn en som handler på impuls (Hutchins, Cloppert, & Amin, 2011). Konsekvensen er at i cyberdomenet er ikke overraskelse nødvendigvis knyttet til militære enheters manøver i øyeblikket, men kanskje til en manøver utført for lenge siden. En realitet som dette gjør at man i et 'worst case scenario' står i fare for å være utmanøvrert før striden har begynt.

3.3 Makt og struktur

Både FFI (2016) og Andreassen (2017) peker på at nettverksbaseringen til nå har gitt lite operativ effekt og at innføringen har gått sakte. Noe av svaret kan kanskje finnes i skillet mellom hierarki og nettverk, og makt. Hierarki betyr sentralisert kommando og kontroll, og sentralisert kommando og kontroll betyr makt. Nettverksbasering og nettverkstenking baserer seg på distribusjon av makt og desentralisert ledelse (FFOD, 2007). I dette grenselandskapet ligger kanskje noe av motsetningen mellom cyberdomenet og ledelse i Forsvaret å finne. To mulige forklaringer belyses:

1. Det å gå fra et veletablert hierarki med godt definert ansvar, roller, myndighet og oppgaver, til et mer løst organisert nettverk, betyr endring. Det kan oppleves som reduksjon i makt (Busch, Vanebo, & Dehlin, 2010). Organisering i mindre enheter på tvers av stridskrefter på tvers av hierarkiet, og til og med til andre sektorer, vil si et redusert handlingsrom dersom man ser på det hele med et konservativt hierarkisk mindset. En mulig løsning på dette problemet kan være å omdefinere den grunnleggende forståelsen av makt, som Naím (2013)foreslår. Dette vil sannsynligvis ikke skje så lenge man fortsetter å utdanne som i dag der "all grunnleggende militær trening og tenkning utgangspunkt i hierarkier." (FFI, 2016, s. 33). Til dels fordi kultur skapes, opprettholdes og endres på Forsvarets utdanningsinstitusjoner (FFI, 2016).
2. En mulig andre forklaring kan være at å gå fra et etablert hierarki til mer dynamisk nettverkstenking kan virke skremmende. Lavere grad av kontroll og høyere grad av usikkerhet knyttet til operasjonelle faktorer vil være realiteten, fordi multi-domene operasjoner vil være mulig (Jøsok et al., 2016). Dette har implikasjoner på hvordan militære lederutdanningen gjennomføres i praksis, og hva som ses på som nødvendig lederkompetanse i et mer dynamisk og komplekst miljø. Kanskje vil det handle mindre om prosedyrer og metoder, og mer enn å håndtere kompleksitet og raske kontekstskifter.

Cyberdomenet som muliggjører for nettverksbasering kan altså oppfattes som en trussel mot personlig makt, og være med på å skape frykt på grunn i overgangen fra hierarkisk tenkning til nettverkstenking. Den økte betydningen av cyberdomenet vil derfor ha konsekvenser for alle domener slik som figur 2 illustrerer, både organisatorisk og individuelt. Når vi tar inn over oss konsekvensen av more, mobility og mentality, er det i denne teksten mest interessant å se på hva dette har å bety for lederskap.

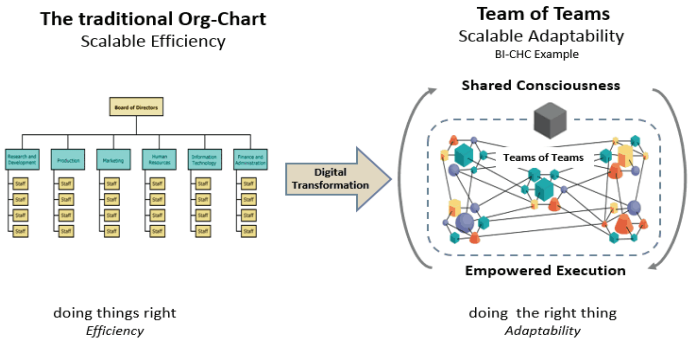
4 Lederskap

4.1 Ledelse av multi-domene operasjoner

Kapittel 2 og 3 har belyst at cyberdomenet skaper utfordringer internt i Forsvarets organisasjon i forhold til at vi må organisere oss annerledes og tenke annerledes, hvis vi skal fungere sammen i og gjennom cyberdomenet. Dette vil kreve nye former for kompetanse (Mld. Stor. Stortingsmelding, 2013). Eksternt skaper cyberdomenet problemer med å distribuere makt til mindre grupper som har evne og vilje til å bruke dette med ondsinnede hensikter. General Stanley McChrystal identifiserte hva dette hadde å si for lederskap gjennom sine erfaringer i Afghanistan: "it became clear to me and to many others that to defeat a networked enemy we had to become a network ourselves." (McChrystal, 2011). I likhet med FFI (2016), påpeker han at den hierarkiske tilnærmingen var uegnet til å håndtere utfordringene han møtte. Megaplayeren NATO kunne ikke hamle opp med micropoweren Al-Qaida. Et grunnleggende problem som McChrystal identifiserte, var motstanderens evne til å organisere seg adaptivt i celler, ofte på tvers av geografi og sammensmeltet med sivilbefolkning. I tillegg hadde motstanderen evne til å utnytte ny teknologi til å dele informasjon raskt og effektivt. Motstanderen viste også stor evne til resiliens, altså å komme seg på beina igjen etter å ha vært slått i et lag. Slik har innsatsen i Afghanistan blitt en dyr affære, som har gitt lite resultat sett opp mot de strategiske målsetningene som var satt for invasjonen. Motstanderen flyttet dermed krigen fra manøverkrigføring som styrkene var forberedt på med store hierarkiske organisasjoner, til counter-insurgency der mindre enheter og andre metoder var mer effektive enn den tradisjonelle krigsmaskinen. For det norske Forsvaret har det vært mange verdifulle erfaringer å hente fra Afghanistan. Men dessverre lite innen ledelse på operasjonelt nivå som Høiback påpeker: "I Norge faller kompetanseforvaltning og kompetanseutvikling utover det stridstekniske nivået utenfor det som vi oppfatter som militært relevant" (Høiback, 2017, s. 33). Norge har definert seg selv som en god alliert (NOU, 2016), men det er neppe nok til å utløse en gjennomgripende debatt som evner å endre lederpraksisen i Forsvaret slik at den kan tilpasses nettverkstenking og fremtidens utfordringer.

4.2 Stormester eller gartner

General McChrystal (2016) beskriver hvordan store organisasjoner må revitalisere seg selv på grunn av den digitale transformasjonen. Uavhengig om det er i næringslivet eller i krig, så identifiserer han at å respondere raskt og det å være tilpasningsdyktig, er kritiske kompetanser i en organisasjon. For å kunne håndtere utfordringene trengs nye kommunikasjonsformer og samarbeidsformer. "That requires new ways to communicate and work together" (McChrystal et al., 2016, s. vii). Konklusjonen til McChrystal er altså nærmest identisk med den FFI (2016) presenterer. McChrystals (2016) visualisering av konklusjoen er også nesten identisk med den FFI (2016) bruker i sin rapport. Cyberdomenet muliggjør nettverksbasering, og tvinger frem en endring fra hierarki til nettverk. Så hva vil dette har å si for lederskap?



Figur 3: Teams of teams (McChrystal et al., 2016)

Nok en gang påpeker McChrystal det som FFI påpeker; man kan ikke utdanne ledere til å fungere i et hierarki når man skal lede i et nettverk, og at dette krever en endring i hvordan ledelse og makt oppfattes. "...the mental transition from heroic leader to humble gardener was not a comfortable one. From the first day at West Point I'd be trained to develop personal expectations and behaviours that reflected professional competence, decisiveness, and self-confidence…. I felt intense pressure to fulfil the role of chess master for which I had spent a lifetime preparing. But the choice had been made for me. I had to adapt to the new reality and reshape myself as conditions were forcing us to reshape our force. And so I stopped playing chess, and I became a gardener" (McChrystal et al., 2016, s. 225).

Konsekvensen av more, mobility og mentality muliggjort av cyberdomenet, gjør verden mer kompleks. Det fører også til at militære operasjoner blir mer komplekse. Det er rett og slett flere faktorer som må tas hensyn til, og disse faktorene er sammenkoblet på nye og komplekse måter. Her er det et viktig skille mellom komplisert og komplekst. Kompliserte problem betyr at det er et relativt oversiktlig sett med variabler som må håndteres i en kontekst. F.eks manøverkrigføring mot en relativt kjent fiende. Komplisert problem som kan løses med å bruke tilgjengelige ressurser effektivt. Komplekst problem krever mer tilpasning, fordi prosedyrene du kan ikke passer til problemet. Derfor kommer McChrystal til konklusjonen at "Adaptability, not efficiency, must become our central competence." (McChrystal et al., 2016, s. 20). Og dette handler om lederskap på flere nivåer. FFI påpeker at det handler om "godt gammeldags lederskap" (FFI, 2016, s. 33). Det betyr ikke at man skal lete frem "Veiledning i militært lederskap fra 1974" og begynne å lese den. Det handler om at alle nivå av ledelse i Forsvaret må innse at lederskap endrer seg i takt med innføring av teknologi og nettverksbasering. Det er ikke effektivt å opprettholde eksisterende maktstrukturer og basere seg på kommando og kontroll i møte med nye utfordringer drevet av f.eks. cyberdomenet. Lederkompetanse er ikke lengre å ha full kontroll på alle stegene og håndverket i alle ledd i organisasjonen. Endringene i Forsvarets organisasjon er allerede for raske til at dette er tilfellet. Lederkompetanse er derfor også i endring. Utfra argumentasjonen i denne teksten er det nødvendig med en dreining mot om å bygge integritet på å gi fra seg makt,

fremfor å sentralisere makt, og dyrke de rundt seg slik at samhandling og kommunikasjon kan finne sted. I en multi-domene kontekst, der domener og dimensjoner smelter sammen, kan vi ikke tillate oss å redusere militært lederskap til en forestilling om at målet er å bli stormester i sjakk.

4.3 Konsekvenser for lederutdanning

Det å gjøre organisatoriske endringer for å tilpasse konsekvenser av cyberdomenets økte betydning, handler i tillegg til organisatoriske og strukturelle endringer, om å ta bevisste valg rundt hvilken kompetanse man tilfører personellet i organisasjonen gjennom utdanning, trening og øving. Det finnes i dag lite beviser på at lederutdanning og lederutvikling fungerer i Forsvaret. Det finnes derimot indikasjoner på det motsatte; at det ikke fungerer, at det er tatt lite bevisste valg og at lederutviklingsstrukturer er redusert (Luktvasslimo, 2013). Et annet eksempel er at kadetter kan beskrives som mindre modne når de uteksamineres enn når de begynner på skole i Forsvaret (Strengen, 2014). Dette kan være en indikasjon på at man prøver å lære bort lederskap som et sett egenskaper, holdninger, ferdigheter og metoder som tilpasses den gjeldende konteksten. Gjerne ved forelesning og deretter praksis hvor man får tilbakemelding på om det er riktig eller feil. Sett i lys av argumentasjonen i denne teksten, fremstår dette som en utdatert forståelse av lederskap, utøvelse av ledelse og det å lære å lede. Feilene her er mange. Forestillingen om manøverkrigføring ligger til grunn for alle militære operasjoner, og man i stor grad forholder seg til stridsteknisk nivå i utdanning av nye ledere. Endringene i cyberdomenet bringer med seg, betyr at nivået må heves (i dobbel forstand) på lederskapsutdanningen tidligere. Først opp fra stridsteknisk til operasjonelt og strategisk, slik at flere ledere forstår koblingen mellom ytterpunktene. Dernest kvalitetsmessig, fra å fokusere på utdaterte kompliserte problem, til komplekse problem som inkluderer stridsfeltets nye realiteter, inkludert cybermakt.

5 Avslutning

Cyberdomenet har en rekke egenskaper som fører med seg endringer og utfordringer som er pekt på i denne teksten. Spesielt er faktorene; more, mobility and mentality belyst. Disse faktorene fører til endrede maktstrukturer som videre har konsekvenser for organisering, og dernest lederskap av militære styrker. Det er vist til at cyberdomenet går på tvers av eksisterende domenene, samtidig som det krysser fysiske, kognitive og informasjons dimensjoner. Bevisst eller ubevisst motstand mot endring, eller evne og vilje til å ta innover seg eller forstå denne realiteten, gjør at nettverksbaseringen av Forsvaret har hatt redusert operativ effekt. Grunnen er at mennesker samhandler og kommuniserer for dårlig innenfor rammen av hierarkiet i en nettverksbasert realitet. Videre argumenteres det for at dette skyldes at maktstrukturer står i fare for å radikalt endres, og at dette dermed kan være en grunn til uvillighet til samhandling, kommunikasjon og nettverkstenking. Videre påpekes det at cyberdomenets inntog har konsekvenser for hvordan vi ser på lederskap konseptuelt, i praksis og i utdanning. Det er

vist til et eksempel der interne erfaringene gjort av FFI i det Norske Forsvaret og eksterne erfaringer gjort av McChrystal i interasjonale operasjoner påpeker samme utfordringer.

Utfordringene militære styrker står ovenfor i tiden fremover, krever at militære styrker organiseres annerledes. Det krever også at personellet tenker annerledes. I denne teksten argumenters det for at dette krever tilpasningsdyktighet foran størrelse og styrke, og at dette har store konsekvenser for lederskap. McChrystal har et godt poeng når han sier at: "There are few secrets to leadership. It is mostly just hard work." (McChrystal et al., 2016, s. 231). Og med dette i tankene, vil jeg påstå at det kreves mye hard tenkning og lite iverksetting for å få lederskap i Forsvaret inn på et fornuftig spor igjen.

6 Referanser

ACT. (2010). *NATO NEC Command and Control Maturity Model*. DoD Command and Control Research Program: Center for Advanced Concepts and Technology Retrieved from http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf.

AJP_3-20. (Draft). *Allied Joint Doctrine for Cyber Operations*. Not Published: NATO.

Allen, S. H., & Machain, C. M. (2017). Understanding the impact of air power. *Conflict Management and Peace Science, 0*(0), 0738894216682485. doi:10.1177/0738894216682485

Andreassen, T. (2017). *The role of trust when implementing Network Based Defence in the Norwegian Armed Forces.* NTNU. Retrieved from http://daim.idi.ntnu.no/masteroppgaver/018/18079/masteroppgave.pdf

Aron, R. (1955). Europe and Air Power. *The ANNALS of the American Academy of Political and Social Science, 299*(1), 95-101. doi:10.1177/000271625529900112

Bibighaus, D. L. (2015). How Power-Laws Re-Write The Rules Of Cyber Warfare. *Journal of Strategic Security, 8*(4), 39-52. doi:http://dx.doi.org/10.5038/1944-0472.8.4.1439

Brangetto, P., & Veenendaal, M. A. (2016). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.* Paper presented at the 8th International Conference on Cyber Conflct, Tallinn.

Buchler, N., Fitzhugh, S. M., Marusich, L. R., Ungvarsky, D. M., Lebiere, C., & Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. *Frontiers in Psychology, 7*(937). doi:10.3389/fpsyg.2016.00937

Busch, T., Vanebo, O. V., & Dehlin, E. (2010). *Organisasjon og organisering* (6 ed.). Oslo: Universitetsforlaget.

FD. (2014). *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren.* Retrieved from

https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf.
FFI. (2016). *Støtte til Forsvarets NbF-utvikling-sluttrapport*. Retrieved from https://www.ffi.no/no/Rapporter/15-02403.pdf
FFOD. (2007). *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben Retrieved from https://brage.bibsys.no/xmlui//bitstream/handle/11250/99256/1/FFOD.pdf.
FFOD. (2014). *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben Retrieved from https://brage.bibsys.no/xmlui//bitstream/handle/11250/99256/1/FFOD.pdf.
Forsvaret. (2012). *Forsvarssjefens grunnsyn på ledelse*. Oslo: Sjef Forsvarsstaben.
Gibney, A. (Writer) & M. S. Alex Gibney (Director). (2016). Zero Days. In M. S. Alex Gibney (Producer).
Haaster, J. v. (2016). *Assessing Cyber Power.* Paper presented at the 8th International Conference on Cyber Conflct, Tallinn.
Høiback, H. (2017). Drømmen om Scharnhorst – om meningers mot. *PACEM, 20*(1), 31-42.
Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80.
Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal Politikk, 71*(02), 241-251 ER.
Jøsok, Ø., Knox, B. J., Helkala, K., Lugo, R. G., Sutterlin, S., & Ward, P. (2016). *Exploring the Hybrid Space Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations.* Paper presented at the 10th International Conference, AC 2016, Held as Part of HCI International 2016, Toronto, ON, Canada.
Luktvasslimo, O. J. (2013). *Ledelse og lederutvikling i Forsvaret. Status og veivalg.*, Bedriftsøkonomisk institutt, Oslo. Retrieved from https://www.regjeringen.no/contentassets/09faceca099c4b8bac85ca8495e12d2d/no/pdfs/nou201620160008000dddpdfs.pdf
Lund, M. S. (2017). Cyber som operasjonsdomene. *Norsk Militært Tidsskrift, 186*(1), 28-34.
McChrystal, S. (2011). It takes a network. The new frontline of modern warfare. Retrieved from http://foreignpolicy.com/2011/02/21/it-takes-a-network/
McChrystal, S., Collins, T., Silverman, D., & Fussell, C. (2016). *Teams of teams: New rules of engagement for a complex world.* New York: Penguin.
MoD. (2013). *Finland's Cyber Security Straregy*. Helsinki: Secretariat of the Security Committee Retrieved from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.
Naím, M. (2013). *The end of power.* New York: Basic Books.
NATO. (2016). Warsaw Summit Communiqué. [Press release]. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

NATO. (2017). Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/cyber-definitions.html

Naughton, J. (2017). North Korea's deadliest weapon? Its hackers. *The Guardian*. Retrieved from https://www.theguardian.com/commentisfree/2017/oct/22/north-korea-deadliest-weapon-cyber-operations-sony-pictures?CMP=share_btn_link

NC3A. (2005). *NATO NETWORK ENABLED CAPABILITY FEASIBILITY STUDY*. NATO Retrieved from http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf.

NOU. (2016). *En god alliert - Norge i Afghanistan 2001–2014*. Oslo Retrieved from https://www.regjeringen.no/contentassets/09faceca099c4b8bac85ca8495e12d2d/no/pdfs/nou201620160008000dddpdfs.pdf.

Perkins, D. G. (2017). Multi-Domain Batte

Driving Change to Win in the Future. *Military Review*. Retrieved from http://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20170831_PERKINS_Multi-domain_Battle.pdf

Stortingsmelding. (2013). *Kompetanse for en ny tid*. regjeringen.no Retrieved from https://www.regjeringen.no/contentassets/16eb33bcb4b847509f9f7b28f7cfbefa/no/pdfs/stm201220130014000dddpdfs.pdf.

Stortingsproposisjon, S. (2016). *Kampkraft og bærekraft*. regjeringen.no Retrieved from https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf.

Strand, T. (2007). *Ledelse, organisasjon og kultur*. (2. utgave ed.). Bergen: Fagbokforlaget.

Strengen, M. (2014). *Virker krigsskoleutdanningen? Norske kadetters personlighetsutvikling gjennom tre år med offisersutdannelse.* (Master of Science), Forsvarets Høgskole, Oslo. Retrieved from https://brage.bibsys.no/xmlui/handle/11250/216611