Fagfellevurdert

Internasjonal POLITIKK
SKANDINAVISK TIDSSKRIFT FOR INTERNASJONALE STUDIER

Årgang 78, Nummer 3, side 362–382, 2020, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert november 2020

Et forsvar i digital krise?

Tormod Heier og Bjørn E. Mobech-Hanssen
Forsvarets høgskole, Norge

Sammendrag

Selv om norske myndigheter ligger på verdenstoppen i digitalisering av offentlige tjenester, står landets forsvar fremdeles «på stedet hvil». I kjernen av problemet finner vi en styringsmodell der 14 ulike forsvarsgrener og selvstendige driftsenheter kjemper om makt og innflytelse. Dette gjelder særlig i spørsmålet om hvem som skal ha ansvar og myndighet når Forsvarets IKT-systemer skal knyttes sammen for å øke cyberberedskapen. Hvordan kan vi beskrive, forklare og forstå de digitale problemene som Forsvaret står oppe i? Nyere forskning gir ikke klare svar, blant annet fordi de fleste studiene er opptatt av å studere utfordringene som kommer utenfra og inn mot Norge. Spørsmålet om hvorfor Forsvaret ikke klarer å forsvare seg mot cyberangrep, eller hvorfor etaten ikke holder tritt med resten av samfunnet, forblir derfor ubesvart. Ved å bruke instrumentelle og kulturelle perspektiver fra organisasjonsteorien finner vi store huller i forsvarsevnen på grunn av intern fragmentering og rivalisering.

Nøkkelord: digitalisering • Forsvaret • digital modenhet • cyberberedskap

I denne artikkelen skal vi beskrive og forklare hvilke utfordringer det norske forsvaret står overfor når etaten må tilpasses et mer digitalt trusselbilde. Hovedargumentet, som i hovedsak er at Forsvaret ikke klarer å oppnå en tilstrekkelig god cyberberedskap, føyer seg inn i en bredere forskningstradisjon der reformer i offentlig sektor står sentralt. På den internasjonale forskningsfronten er offentlig reformarbeid et hett

*Kontaktinformasjon: Bjørn E. Mobech-Hanssen, e-post: bmobechhanssen@fhs.mil.no

Citation: Heier, T. & Mobech-Hanssen, B. E. (2020). Et forsvar i digital krise? Internasjonal Politikk, 78(3), 362–382. http://dx.doi.org/10.23865/intpol.v78.2288

tema. Ettersom stadig flere land knytter samfunnskritisk infrastruktur tettere opp til globale nettverk, blir de også nødt til å endre praksis (se blant annet Colombo, Dagnio, Lehmann & Salmador, 2019; Cunningham, Menter & Wirsching, 2019). Mye av den internasjonale forskningen retter seg derfor inn mot dilemmaer som oppstår i arbeidet med økt cyberberedskap. Eksempler på dette kan være balansen mellom standardisering og variasjon, brukervennlighet og redundans, eller mellom kosteffektivitet og robusthet (Flyverbom, Deibert & Matten, 2019; Wareham, Fox & Giner, 2014). Under slike forhold må moderne stater hensynta samfunnsmessige forventninger om bedre tjenester gjennom digitalisering. Samtidig som statene også må bygge beredskap mot uønskede forstyrrelser, degraderinger eller sågar angrep mot den digitale infrastrukturen (Flyverbom, Deibert & Matten, 2019; Wareham, Fox & Giner, 2014).

I Norge har statsforvaltningen jobbet aktivt for å gi innbyggerne gode digitale tjenestetilbud, samtidig som sikkerheten ivaretas. Ifølge Statistisk sentralbyrå (Røgeberg, 2019) er landet blant verdens beste når det gjelder bruk av digitale tjenester. Siden 2009 har det vært en jevn økning i befolkningen som bruker offentlige nettjenester, og Norge er på europatoppen (sammen med Finland) når det gjelder digital samhandling mellom borger og stat (Eurostat, 2019). Satsingen har bidratt til at norsk digital infrastruktur er blant verdens beste, noe som igjen har gitt offentlig og privat sektor betydelige konkurransefortrinn i forhold til andre land (Digi.no, 2017). Dette bildet samsvarer med Solberg-regjeringens ambisjoner, der «Norge skal ha verdens beste digitale tjenester og en offentlig sektor som legger til rette for innovasjon og nyskaping» (Kommunal- og moderniseringsdepartementet, 2018).

Samtidig står norske myndigheter på stedet hvil når det gjelder cyberberedskap i landets væpnede styrker. Ifølge sjefen for det norske Cyberforsvaret (CYFOR), generalmajor Inge Kampenes, har forsvarsledelsen ingen mulighet til å stå imot utenlandske cyberangrep (Eide & Nørstebø, 2017): «Vi er marginale på hele spekteret av oppgaver – fra oppfylling av beredskapsbeholdning til styrkestruktur og planverk. […] Hvis det pøses på med cyberangrep mot oss vil vi ikke holde lenge». Manglende cyberberedskap gir dermed inntrykk av en etat som lider av digital umodenhet. Dette er oppsiktsvekkende all den tid Forsvarets egen etterretningstjeneste, samt Politiets sikkerhetstjeneste (PST), fremhever cybertrusler som de mest alvorlige utfordringene mot landet (Etterretningstjenesten, 2020; PST, 2020). Mens Nasjonal sikkerhetsmyndighet (NSM) ifølge sikkerhetsloven har ansvaret for den digitale infrastrukturen på sivil side, har Forsvaret ansvaret for den militære cyberberedskapen. Like fullt understreket daværende forsvarssjef Haakon Bruun-Hanssen (2013–2020) i sitt fagmilitære råd til Solberg-regjeringen at Forsvarets digitale modenhet måtte styrkes. Hvis ikke, ville landets styrker «miste avgjørende kampevne tidlig» i krise eller krig (Forsvaret, 2019).

Med unntak av Riksrevisjonen (2011) og McKinsey & Co. (2015) er etatens digitaliseringsproblemer sterkt underkommunisert. Dette kan kanskje bety at det norske forsvaret så langt ikke har blitt utsatt for alvorlige cyberangrep som har

kommet offentligheten for øre. Risikoen for slike angrep er imidlertid økende, all den tid norske styrker stadig oftere trekkes inn i den pågående stormaktsrivaliseringen mellom USA og Russland i nordområdene. Norges militære infrastruktur kommer dermed også høyere opp på Russlands liste over aktuelle mål som eventuelt bør påvirkes i en eventuell krise eller krig. Dette er ikke fordi Russland frykter militære angrep fra norske styrker, men fordi norsk territorium og norsk militær infrastruktur kan bli brukt som utgangspunkt for amerikanske operasjoner inn mot Russland (Heier, 2019, s. 35, 45–52). Derfor er det også viktig med mer kunnskap på dette fagfeltet. Flere stortingsrepresentanter hevder nemlig at manglende cyberberedskap i Forsvaret «er ukjent farvann», og at «vi ikke har stor nok oppmerksomhet rundt dette»; det innrømmes også at norske myndigheter «springer litt etter» når det gjelder å forstå omfanget av Forsvarets cyberproblemer (Elvenes, Sivertsen & Skotåm, 2019).

Hovedspørsmålene vi stiller er derfor todelt: *Hvordan kan Forsvarets digitale modenhet best beskrives? Og hvordan kan det digitale etterslepet forstås mer allment?* Implisitt i det første spørsmålet ligger metodespørsmålet om hvilke indikatorer som er best egnet til å beskrive den digitale modenheten. Det andre spørsmålet, derimot, kan besvares mer konkret ved hjelp av to delspørsmål fra organisasjonsteorien: Kan Forsvarets digitale etterslep forstås i lys av etatens styringsmodell, der 14 ulike forsvarsgrener og selvstendige driftsenheter skal forsøke å bli enige om hvilke digitale løsninger som er best for dem selv?[1] Eller kan det være at kulturelle årsaksforhold spiller inn, fordi uformelle praksisfellesskap innad i forsvarsgrenene og driftsenhetene skaper motkrefter som hemmer helhetlige digitale fellesløsninger?

Det finnes ingen forskningsbasert kunnskap som på systematisk vis analyserer hvorfor Forsvaret henger etter resten av samfunnet på det digitale området. Det har riktignok vært forsket en hel del på digitale problemer, blant annet om hvordan internettet kan forstås som en «geopolitisk arena» (Svenungsen, 2019) og hvilke konsekvenser dette kan få for Norge (Johnsen, 2013). Betydningen av militær avskrekking i et «forsvar av cyberspace» føyer seg inn i rekken av nyttig kunnskap (Kristiansen & Hoem, 2019; Muller, 2019). Det samme gjør arbeider med nordiske lands erfaringer med «cyberresiliens, sektorprincip og ansvarsplacering» (Jensen, 2019), der digitaliseringsproblemene i Nord-Europa analyseres mer allment. Dette er viktige arbeider for å forstå hvordan forstyrrelser eller sågar angrep mot samfunnskritisk infrastruktur undergraver politisk styringsevne i små, åpne og velutviklede – men

[1] Driftsenhetene i Forsvaret har egne budsjetter og kompetansemiljøer slik at de kan løse ulike deloppgaver i forsvaret av Norge, hjemme så vel som i utlandet. Driftsenhetene er spredt rundt om i landet, men lederne møtes i Forsvarssjefens ledergruppe i Oslo og representerer følgende enheter: Hæren, Sjøforsvaret, Luftforsvaret, Heimevernet, Cyberforsvaret, Forsvarets spesialstyrker, Etterretningstjenesten, Forsvarets operative hovedkvarter, Forsvarets logistikkorganisasjon, Forsvarets sanitet, Forsvarets høgskole, Forsvarets fellestjenester og Forsvarets personell- og vernepliktsenter (Forsvaret, 2020).

også svært sårbare – demokratier. Arbeidene gir imidlertid få svar på hvorfor det norske forsvaret ikke klarer å tilpasse seg truslene som Etterretningstjenesten og PST advarer mot. Spørsmål om hvordan Forsvarets formelle organisering eller uformelle forsvarsgrenvise praksisfellesskap påvirker den militære cyberberedskapen forblir dermed ubesvart.

De to hovedspørsmålene besvares på følgende måte. Først søker vi svar på hvilke indikatorer som er best egnet til å forstå begrepet «digital modenhet». Deretter bruker vi disse indikatorene til å beskrive situasjonen i Forsvaret. Etter dette presenteres en organisasjonsteoretisk modell som brukes til å tolke og forstå det digitale etterslepet. Avslutningsvis utledes en konklusjon som bygger på de instrumentelle og kulturelle årsaksforholdene vi har belyst i analysen.

Først må imidlertid «digitalisering» defineres og kildebruken drøftes. «Digitalisering» er et verb som beskriver en transformativ prosess, altså en gjennomgripende endring i måten organisasjonens viktigste oppgaver løses på. Fra å anse IKT-systemer som et støtteverktøy som tvinges inn i den eksisterende organisasjonen, forstår vi det motsatte: at IKT-systemene tvinger organisasjonen og de ansatte til å løse organisasjonens viktigste oppgaver på nye måter. Hensikten med dette er å nyttiggjøre seg det hele og fulle potensialet som ligger i IKT-systemene. Digitalisering oppstår altså når de ansatte klarer å utnytte IKT-systemenes fulle potensiale fremfor å tviholde på organisasjonens opprinnelig form og arbeidsmåte (Westerman, Bonnet & McAfee, 2014).

Denne forståelsen er blant annet basert på kunnskap fra seks nøkkelinformanter med unik kunnskap om Forsvarets cyberberedskap. Informantene har bekledd så vel sjefsstillinger i CYFOR som mellomlederstillinger i CYFORs planstab og våpenskole. De andre informantene er en professor i informasjonssikkerhet ved Cyberingeniørhøgskolen, samt en avdelingsdirektør og en senior stabsoffiser sentralt plassert i Forsvarsstabens styringsavdeling. Dermed fanger vi inn forskningsbaserte og erfaringsbaserte perspektiver, men også lederperspektiver og brukerperspektiver fra ulike kommandonivåer og ulike underavdelinger innenfor og utenfor CYFOR. Dette er ikke det samme som å si at det ikke finnes andre synspunkter. I et forsvar med 14 driftsenheter og 17 000 ansatte vil det til enhver tid finnes utallige synspunkter som det vil være vanskelig å kartlegge fullt ut. Denne ulempen kan best beskrives med sitatet til den amerikanske organisasjonsteoretikeren Graham Allison: «where you stand depends on where you sit» (Allison & Zelikow, 1971). Informasjonen fra intervjuobjektene er derfor understøttet av skriftlig dokumentasjon fra Forsvarets egen saksbehandling: dels gjennom en unik cyberutredning med representasjon fra de mest sentrale driftsenhetene (Forsvaret, 2019); dels gjennom etatens egen strategi, *Forsvarets digitaliseringsstrategi* (Forsvaret, 2018). Og til sist, gjennom fagmilitære anbefalinger til regjeringen. I tillegg er det brukt foredrag og uttalelser i mediene, primært fra CYFOR-ledelsen, samt relevant forskningslitteratur. Samlet sett kan dette gi et godt bilde av cybermiljøenes «indre liv», uten at bildet nødvendigvis dekker alle nyansene i Forsvarets digitale sakskompleks.

Hvordan kan Forsvarets digitale modenhet beskrives?

Eksakte kriterier for digital modenhet er vanskelig å utlede; for hvordan måles modenhet?

Ved å trekke veksler på forskningen som er gjort innenfor temaet «kapasitetsbygging på cybersikkerhet» (*cybersecurity capacity*), kan den britiske modellen til William H. Dutton, Sadie Creese, Ruth Schillair og Maria Bada brukes. I modellen, som ble utviklet ved Oxford Martin School i 2019, er det særlig tre variabler som vektlegges. Den første variabelen er «aktørmangfold», som er brutt ned i en rekke organisatoriske underenheter. Blant de viktigste er: (i) beslutningstakere som gir retning for organisasjonens digitale virksomhet; (ii) ansatte som bruker digitale løsninger; (iii) donorer med ansvar for innkjøp, drift og vedlikehold (Dutton et al., 2019, s. 284–5). Den andre variabelen er «kapasitetsbyggingens brede og sammensatte nedslagsfelt». Variabelen er operasjonalisert til et sett med indikatorer som blant annet krever innføring av (i) ny IKT (*high quality software*), (ii) bygging av sterk sikkerhetskultur og (iii) kompetansebygging i egen organisasjon slik at kunnskaper, ferdigheter og holdninger skjerpes (*supporting awareness and good practice*) (Dutton et al., 2019, s. 283–284). Den tredje variabelen er «policy og praksis», som krever sterke samordningsmekanismer; dels mellom (i) mange enkeltstående aktører som hver for seg skal løse særegne arbeidsoppgaver (*a multiutude of actors*), men også (ii) overlappende arbeidsområder der grensene mellom hvem som gjør hva er uklare (*interrelated policy domains*) (Dutton et al., 2019, s. 287).

Om vi sammenligner de tre variablene med *Forsvarets digitaliseringsstrategi* fra 2018, ser vi at suksesskriterier for «digital modenhet» langt på vei sammenfaller med flere av de britiske indikatorene. Forsvarets digitale modenhet defineres langs fem variabler. Først, en «organisatorisk styringsmodell» som, i likhet med det britiske «aktørmangfoldet», består av mange organisatoriske underenheter, der noen gir ut overordnede retningslinjer for forsvarsgrenenes digitale utvikling, mens andre er brukere eller donorer med ansvar for innkjøp, drift og vedlikehold. Dernest, «innføring av ny teknologi for å effektivisere verdikjeden og oppdragsporteføljen». Denne variabelen fanger opp den britiske modellens vektlegging av *adopting, procuring, and deploying high quality software*. Så følger «bedre informasjonssikkerhet», som i grovt samsvarer med *high quality software*. Dernest følger «mer digital kompetanse blant de ansatte», som fanger opp indikatoren *supporting awareness and good practice*. Til sist kommer «tettere samhandling mellom avdelinger som til daglig har ulike oppgaver» (Forsvaret, 2018), noe som gjenspeiler den britiske modellens fokus på *a multitude of actors* og *interrelated policy domains*.

Den begrepsmessige validiteten mellom den britiske modellen og *Forsvarets digitaliseringsstrategi* er langt fra perfekt. Dette kan blant annet skyldes at Forsvarets omgivelser er svært ulike de omgivelsene som den britiske modellen er myntet på. Forsvarets variabler er laget med tanke på trusler og militære mottiltak; de britiske variablene er naturlig nok mer innrettet mot fredstidsdrift i sivile organisasjoner.

Likevel synes det å være flere likheter enn ulikheter. På tvers av Nordsjøen ser vi at begge enhetene vektlegger digitale arbeidsmetoder, effektive verdikjeder, digital kompetanse og samarbeid mellom enheter som i utgangspunktet har ulike oppgaver. Samsvaret gir derfor tilstrekkelig god pålitelighet for å beskrive digital modenhet langs et sett av mer eller mindre allmenngyldige egenskaper. Forsvarets kriterier kan med andre ord sies å være representative til et større univers av sammenlignbare størrelser (Jacobsen, 2010, s. 89). Dermed kan vi også feste lit til hva Forsvaret selv legger i begrepet «digital modenhet», og hvordan vi selv forstår begrepet. Hvordan kan så den digitale modenheten i Forsvaret beskrives?

Digitalisering til besvær

Ifølge *Forsvarets digitaliseringsstrategi* beskrives forsøkene på å innføre ny teknologi som svært vanskelig. I strategien erkjennes det at «Forsvaret henger etter samfunnet for øvrig, […] at den digitale modenhet er lav, og at utviklingen av nye løsninger tar for lang tid» (Forsvaret, 2018).

Når det gjelder variabelen *styringsmodell* vektlegger digitaliseringsstrategien raskt å få på plass en såkalt «omforent virksomhetsarkitektur» mellom 14 ulike forsvarsgrener og driftsenheter. Dette betyr å innføre et mer helhetlig styringskonsept der enhetene ikke bare er opptatt av egen kjernevirksomhet, men å sette egne oppdrag inn i et mer helhetlig styringssystem. Digitale reformtiltak, fra for eksempel Forsvarsstaben i Oslo eller CYFOR på Lillehammer, må følgelig få konsekvenser for måten Luftforsvaret på Rygge, Hæren i Bardufoss eller Sjøforsvaret i Bergen løser oppdragene sine på. Ifølge digitaliseringsstrategien vil dette kreve et betydelig løft: dels i måten Forsvaret driver kompetanseheving på, men også i måten forsvarsgrenene samarbeider på, og i måten driftsenhetene balanserer egne og overordnede behov på (Forsvaret, 2018).

Når det gjelder variabelen *teknologi* ser også denne situasjonen ut til å være alvorlig. Dette skyldes, ifølge Forsvaret selv, at innføringen av nye og forvaltningen av gamle IKT-systemer er svært vanskelig. Ifølge tidligere sjef CYFOR, generalmajor Odd-Egil Pedersen (2013–2017), finnes det i dag nærmere 200 IKT-systemer rundt om i Forsvaret som ikke kommuniserer med hverandre (Heier, 2018, s. 305). Dermed skapes det ikke synergi mellom militære avdelinger som i utgangspunktet var ment å gi hverandre gjensidig støtte i møtet med fienden. Manglende samhandling skaper store sårbarheter fordi knappe ressurser verken kan kraftsamles eller settes inn der trusselen er størst. Problemet ble åpent adressert i 2015 under et foredrag i Oslo Militære Samfund. Her advarte generalmajoren sine kollegaer fra luft-, sjø- og landdomenet om at kampenhetene deres kunne ikke kommunisere med hverandre, selv ikke når de befant seg i det samme operasjonsområdet. Enda verre var det at selv våpensystemer fra en og samme forsvarsgren heller ikke kunne gi hverandre gjensidig støtte (Pedersen, 2015). Det digitale beredskapsproblemet er også synlig i *Forsvarets digitaliseringsstrategi*: «uklar rollefordeling, duplisering og uløste oppgaver» fremheves spesielt (Forsvaret, 2018).

Situasjonen innen *informasjonssikkerhet* kan, ifølge Forsvarets egen toppledelse, også beskrives som alvorlig. Det empiriske belegget for denne beskrivelsen er allerede antydet i innledningen, der sjef CYFOR, generalmajor Inge Kampenes, i et intervju med *Forsvarets Forum* hevdet at Forsvaret er «marginale på hele spekteret av oppgaver – fra oppfylling av beredskapsbeholdning til styrkestruktur og planverk» (Eide & Nørstebø, 2017). Dette støttes også av uttalelser fra CYFORs kommunikasjonssjef, Knut Grandhagen, som to år senere hevdet at Forsvaret fremdeles «mangler et effektivt system for raskt å identifisere og håndtere store hendelser» (Tømmerbakke, 2019). Ifølge den interne Cyberutredningen som bistod i Forsvarssjefens militærfaglige råd til forsvarsministeren høsten 2019, hevdes det sågar at «dagens informasjonsinfrastruktur ikke er forsvarbar»; Forsvaret har liten evne til å «utlede handlemåter for beskyttelse» av sine IKT-systemer (Forsvaret, 2019, s. 21). Alvoret forsterkes ytterligere ved at militære avdelinger som skal forsvare Norge bruker «IKT-systemer som eies og driftes av sivile virksomheter (underleverandører til Forsvaret)». Disse løsningene er imidlertid ikke laget for å virke «under ekstreme forhold, som i krise og krig» (Forsvaret, 2019, s. 15). *Forsvarets digitaliseringsstrategi* erkjenner denne sårbarheten, og understreker behovet for mer «informasjonssikkerhet i anskaffelser og utvikling av fremtidig sikkerhetsarkitektur» (Forsvaret, 2018).

Når det gjelder variabelen *digital kompetanse*, kan situasjonen beskrives som vanskelig. Ifølge Cyberutredningen er det store mangler rundt om i den militære kommandokjeden. Selv om stadig flere fly, båter og kjøretøyer knyttes opp til digitale nettverk i egne forsvarsgrener, er viljen til å bygge kompetanse, utvikle planverk og øve på beskyttelse mot cybertrusler liten. Dermed blir det heller ikke utviklet realistiske bilder av hvilke sårbarheter norske styrker står overfor. Dette skyldes i stor grad at de forsvarsgrenvise kompetansemiljøene i Hæren, Luftforsvaret og Sjøforsvaret ikke prioriterer cybersikkerhet og cyberoperasjoner. Til tross for spede forsøk fra forsvarsgrenene på å integrere cyberoperasjoner i trening og øving, var så vel Forsvarssjefen som sjef CYFOR og arbeidsgruppen bekymret: Forsvarets innsats var fragmentert og sporadisk, og mannskapene mangler nødvendig kompetanse. Kvaliteten på «cyber-spill under øvelsene var lav og problemstillinger håndteres på et svakt militærfaglig grunnlag» (Forsvaret, 2019, s. 17). Svakhetene ble også adressert i *Forsvarets digitaliseringsstrategi*: «den digitale kompetansen må heves»; «ledere og ansatte må forstå de teknologiske driverne og evne å sette en retning som utvikler organisasjonen» (Forsvaret, 2018).

Innenfor den siste variabelen, *samhandling*, erkjenner Forsvaret at det daglige samarbeidet mellom driftsenhetene må styrkes. Dette gjelder for så vel operative som forvaltningsmessige oppgaver (personell, økonomi og logistikk), og på tvers av etatsvise og allierte grensesnitt. *Forsvarets digitaliseringsstrategi* legger særlig vekt på verdikjeden innenfor tradisjonelt HR-arbeid, samt informasjonsdeling mellom forsvarsgrener og driftsenheter. Ifølge strategien er dagens verdikjeder for lange og for kompliserte. Dette gjør at forsvarsansatte bruker uforholdsvis mye ressurser på administrasjon. Dermed forsvinner viktig tid som ellers skulle blitt brukt til de verdiskapende oppgavene som

har med forsvaret av landet å gjøre (Forsvaret, 2018). Et eksempel på dette er Forsvarets arkivtjeneste. I samtalene med professor i informasjonssikkerhet, Mass Soldal Lund fra Cyberingeniørhøgskolen, bruker de ansatte i gjennomsnitt cirka syv minutter på hver e-post som skal journalføres. Dette er fordi epostene må overføres fra det åpne nettet til det begrensede forsvarsnettet FIS Basis (intervju 16.3.20).

Et forsvar i digital krise

At Forsvaret lider under lav digital modenhet synes å være en rimelig beskrivelse av situasjonen. Langs de fem variablene styringsmodell, teknologi, informasjonssikkerhet, kompetanse og samhandling er det identifisert fundamentale sårbarheter. Det er grunn til å feste lit til funnene: Datagrunnlaget er hentet fra primærkilder som befinner seg sentralt i Forsvarets ledelse og i CYFOR. Vi må derfor anta at de ulike kildene, herunder intervjuobjektene så vel som utredningene og digitaliseringsstrategien, gir oss førstehåndskunnskap om problematikken. Kildene kaster også et ærlig, åpent og særdeles usminket lys over situasjonen. Kildene samsvarer også godt med den svært så kritiske konsulentrapporten som McKinsey & Co. laget for Forsvarsdepartementet i 2015 (McKinsey & Co., 2015, s. 51–66). Beskrivelsene langs de fem variablene er i tillegg tuftet på flere av de samme indikatorene som brukes internasjonalt, blant annet ved Oxford Martin School i Storbritannia.

Beskrivelsen gir oss derfor grunn til å hevde med nokså stor sikkerhet at det norske forsvaret befinner seg i en dyp digital krise. Ved å bruke det norske digitaliseringsdirektoratets kriterier for *Vurdering av digital modenhet* for statlige virksomheter, faller Forsvaret inn i kategorien «uformell og tilbakelent» (Røise, 2017). Forsvaret fikk riktignok karakteren «meget god» av Solberg-regjeringen når det gjaldt militær virksomhet i utlandet. På hjemmebane, derimot, i forsvaret av Norge, var karakteren så vidt over stryk – «mindre god» (Forsvarsdepartementet, 2018, s. 55). Slike karakterer kan ofte være unyanserte og gi et fortegnet bilde av situasjonen. Kritikken fra departementet føyer seg imidlertid inn i et bredere mønster, som også innbefatter cyberberedskapen til Forsvaret. Ifølge underdirektør Jan Vidar Moen i Forsvaret ga Forsvarsdepartementet karakteren 2,5 (der 6 var toppkarakter) når Forsvarets digitale modenhet skulle beskrives (Moen, 2019). Innad i Forsvarsstaben, derimot, var oppfatningen mer positiv. Informantene vi intervjuet oppga selv karakteren 2,9 som mer treffende (intervju med Berg og Gulliksen, 9.3.20).

Hvordan kan vi mer allment forstå den digitale krisen som Forsvaret befinner seg i? I resten av artikkelen gjør vi tre ting: først presenteres en forklaringsmodell som gjør det mulig å tolke den svake cyberberedskapen. Deretter analyseres empirien i lys av modellen, før det utledes en konklusjon.

Hvordan kan digitale etterslep forstås?

For å forstå hvilke krefter som påvirker Forsvaret, kan organisasjonsteoretiske perspektiver være nyttige. Skoleretninger med størst forklaringskraft antas å komme fra

de instrumentelle perspektivene til blant annet Olsen (1988), Bouckaert, Peters og Verhoerst (2010) og Christensen (2017), samt institusjonelle perspektiver fra blant andre Thompson (2007); Selznick (1957); March & Olsen (1989). Det instrumentelle perspektivet gir grunn til å anta at lav digital modenhet skyldes måten Forsvaret er organisert på. Med andre ord, at Forsvarets innretning eller styringsmodell (den uavhengige variabelen) har en negativ effekt på etatens digitale modenhet (den avhengige variabelen). Men det kan også være at det finnes viktige nyanser som ikke fanges opp i det instrumentelle perspektivet. Vi vil derfor undersøke om også uskrevne praksisfellesskap og kollegiale nettverk innad i forsvarsgrenene kan ha betydning. For å kaste mer lys over problemet trekkes derfor også kultur inn som uavhengig variabel.

Instrumentelle forklaringer

Det norske forsvaret er, som de fleste andre byråkratiske organisasjoner, preget av hierarki, arbeidsdeling, regler og prosedyrer. Dette er i tråd med Max Webers syn på statlige organisasjoner: et rasjonelt, toppstyrt og upersonlig instrument som brukes for å løse statens oppgaver. Målene som settes er klart definerte og løses ut ifra en rasjonell mål-middel-analyse. Den instrumentelle logikken kommer dels til uttrykk gjennom vertikal samordning nedover i styringskjeden, men også gjennom horisontal samordning med sideordnede enheter (Bouckaert et al., 2010, s. 24).

Dette betyr at hierarkiske organisasjoner som Forsvaret lett utsettes for krysspress mellom vertikal spesialisering og horisontal samordning. Dette gjelder særlig i spørsmål om hvordan store og små problemer, som for eksempel digitaliseringsproblemet i etaten, skal løses. Hierarkiske organisasjoner har nemlig en liten toppledelse, med begrenset kapasitet og spisskompetanse. Ledergruppen er derfor ikke selv i stand til å løse problemene, noe som gjør at arbeidsoppgaver må fordeles og delegeres nedover i systemet. Følgelig må også makt og myndighet delegeres slik at underenhetene får nødvendig gjennomføringskraft til å løse oppgavene.

Men spredning av makt, myndighet og kompetanse kan også føre til friksjon og uenighet: vertikalt, mellom organisasjoner som befinner seg på ulike nivåer i kommandokjeden. Og horisontalt; mellom sidestilte enheter som riktignok skal ta helhetlige beslutninger, men som også skal løse egne kjerneoppgaver. Ut ifra denne logikken kan vi anta at beslutningsprosessene i Forsvaret preges av maktkamp og rivalisering mellom sterke forsvarsgrener og driftsenheter på samme nivå i organisasjonen (Christensen, 2017, s. 61–65). Samtidig vil det også forekomme forhandlinger og kompromisser. Organisasjonen må tross alt forsøke å komme seg videre, uten å fremstå som handlingslammet eller ødelagt av interne konflikter (Olsen, 1988). Konsekvensen er uansett at denne type organisasjon raskt preges av en form for begrenset rasjonalitet. Dette er fordi arbeidsfordeling ofte fører til mer spesialisering og autonomi, som igjen gjør at smalere særinteresser ofte får forrang fremfor bredere og mer overgripende fellesløsninger. I tillegg vil enhetene som befinner seg lenger nede i organisasjonen ikke ha det samme overblikket som enhetene høyere oppe i

systemet. Dette kan gjøre det vanskelig for ledergruppen å få med seg de ansatte på helhetlige fellesløsninger.

Hvilke empiriske forventninger kan vi så utlede fra dette? For vårt vedkommende kan vi forvente at Forsvaret vil preges av maktkamper og kompromisser. Dette gjelder dels mellom CYFOR, forsvarsgrenene og Forsvarets operative hovedkvarter, men også opp imot Forsvarets logistikkorganisasjon og den eksterne etaten Forsvarsmateriell. Dette er fordi det er vanskelig for 14 ulike driftsenheter å bli enige seg imellom, særlig i spørsmål om hva som er best når en helhetlig digital infrastruktur skal knytte driftsenhetene sammen med ett nervesystem.

Hvorvidt den empiriske forventningen leverer gyldige analyseresultater, avhenger blant annet av nøkkelbegrepenes operasjonalisering (Jacobsen, 2010, s. 236–237). I denne sammenheng bruker vi «maktkamp og kompromiss» som utgangspunkt for å tolke og forstå datagrunnlaget. Vi foreslår følgende operasjonalisering på de to begrepene: en fragmentert toppledelse, sterke forsvarsgrenvise særinteresser, og et tilsvarende fravær av helhetlig og overordnet styring.

Kulturelle forklaringer

Det er mange fordeler med instrumentelle organisasjoner, men det finnes også ulemper. En av disse er, ifølge den amerikanske sosiologen James D. Thompson (1920–1973), at organisasjoner som tuftes på arbeidsdeling også utvikler subkulturer. Dette gjelder spesielt når makt og myndighet delegeres nedover i linjen, til underenheter som til daglig ikke har så mye med hverandre å gjøre (Thompson, 2007, s. 140–143). Forsvarets ulike driftsenheter kan tolkes i dette perspektivet. Gjennom særegne karriereplaner, utdanningsdirektiver og doktriner utvikles egne identiteter, rettesnorer og moralske «kompass». Dette er uformelle «sånn-gjør-vi-det-her»-regler som underavdelingene lenger nede i organisasjonen oppretter, videreutvikler og forsterker. For Forsvarets vedkommende kan dette være luft-, sjø- og landmilitære staber, krigsskoler og karriereplaner. Hva som er militærfaglig «rett» og «galt», hva det er verdt å samarbeide med andre om, og hvordan fellestenkning skjer på tvers av luft-, sjø-, land- og cyberdomenet, påvirkes av i stor grad av hvordan forsvarsgrenene selv opplever situasjonen.

Dette gjør at vi også må trekke kulturelle årsaksforhold inn i analysen, ikke minst for å få frem flere nyanser enn hva det instrumentelle perspektivet klarer alene. Forsvarsetaten er nemlig ikke bare et toppstyrt verktøy for politikernes rasjonelle mål-middel-kalkyle. Ifølge Selznick (1957, s. 20) finnes det «[…] et internt sosialt miljø som også må ivaretas». Alle organisasjoner lever sine egne liv der uskrevne normer, regler og forventninger legger føringer for hva som er akseptabel adferd blant de ansatte. Disse uformelle adferdsmønstrene utgjør selve kulturen i enhver organisasjon. Kultur er imidlertid et diffust begrep, med et vidt meningsinnhold. I denne modellen forstås kultur som «[…] a fairly stable set of taken-for-granted assumptions, shared beliefs, meanings, and values that form a kind of backdrop for action» (Smircich, 1985, s. 58). Dermed får tidligere etablerte normer og tradisjoner

betydning for hvordan vi tolker og forstår organisasjoners adferd (Christensen et al., 2017). Særegne doktriner og prosedyrer, men også uskrevne tommelfingerregler og forventninger om hva som bør gjøres i spesifikke situasjoner, vokser frem; gjerne langt nede i organisasjonen der behovet for kompromiss og forhandling mellom balanserte og overordnede hensyn ikke er like sterkt. Snarere blir det viktigere med lojalitet og samhold i primærgrupper, kollegiale nettverk og særegne profesjonsfellesskap som utvikles seg i trygg avstand fra maktens sentrum (Thompson, 2008). Eksempler på dette er forsvarsgrenenes militærfaglige tyngdepunkter, som for Luftforsvarets del ligger på Rygge, mens Hæren og Sjøforsvaret er forlagt på henholdsvis Bardufoss og i Bergen.

I slike institusjoner vokser det frem særegne meningsfellesskap fordi ansatte sosialiseres inn i bestemte måter å forstå verden på. Slike sosialiseringsprosesser skaper stiavhengighet, ofte med tydelige «fødselsmerker» fra organisasjonens fortid (Christensen et al., 2017, s. 61–64). Dette er hva James G. March og Johan P. Olsen (1989) kaller *historisk ineffektivitet*. I realiteten betyr dette at store organisasjoner tidvis vil ha problemer med å følge med i tiden, særlig når nye teknologier, arbeidsmetoder eller utfordringer dukker opp i horisonten (Christensen et al., 2017, s. 62).

Hvilke empiriske forventninger kan vi utlede fra dette perspektivet? I tråd med beskrivelsen over må vi anta at digitale etterslep langt på vei skyldes motstand fra sterke subkulturer innenfor Forsvarets egne rekker. Med dette menes at det innad i Forsvaret finnes underenheter som styres av særegne normer og oppfatninger, og at disse utløses når ny IKT utfordrer måten eksisterende kjerneoppdrag løses på. Mer konkret snakker vi om luft- sjø- og landmilitære enheter som holder til rundt om i landet; kompetansemiljøer som er tuftet på sterke kollegiale nettverk og militære praksisfellesskap. Innenfor egen forsvarsgren eller driftsenhet står enhetene sterkt. Riktignok ikke ut ifra hva som tjener Forsvaret best, men ut ifra hva som er best for egen avdeling eller forsvarsgren.

Kollegiale nettverk og militære praksisfellesskap er, i likhet med maktkamp og kompromiss, upresise begreper. Hvordan gjør vi dem målbare? Ved hjelp av logikken om «stiavhengighet» og «kulturelt passende adferd» legger vi vekt på følgende institusjonelle trekk: En sterk, forsvarsgrenvis forankring der egen praksis bygger på lojalitet, samhold og disiplin. Men også på ulike former for konservatisme, rigiditet og innadvendthet når egen avdeling står overfor bredere og mer gjennomgripende endringer.

En instrumentell fortolkning

Forsvarets digitaliseringsstrategi synes å vektlegge problemer rundt egen styringsmodell. Å få 14 forskjellige forsvarsgrener og driftsenheter til å gå i takt når nye digitale verktøy skal tas i bruk er vanskelig. Dette er fordi én enkelt driftsenhet, som for eksempel CYFOR på Lillehammer, ikke har nok myndighet til å få gjennomslag hos de andre driftsenhetene i etaten. Eksempler på dette kan være overfor Forsvarets

operative hovedkvarter, eller overfor Forsvarsmateriell (som er skilt ut som egen etat i forsvarssektoren). Arbeidsdeling og delegering av makt og myndighet mellom CYFOR og de andre driftsenhetene skaper friksjon og samordningsproblemer. Dette skyldes, ifølge tidligere sjef for CYFOR generalmajor Odd Egil Pedersen, at det ikke er klare grenser mellom hva som er et klart cyberansvar, og hva som er et klart logistikk-, forsvarsmateriell- eller luft-, sjø- og landansvar (intervju, 18.3.20). Dermed svekkes Forsvarets cyberberedskap, fordi grenspesifikke nettverksløsninger ikke knyttes sammen eller ses i sammenheng. Da blir det svært vanskelig, ifølge Pedersen, å samordne en felles forsvarsinnsats i tid og rom (intervju, 18.3.20).

Et eksempel på uklare ansvarsforhold er Forsvarets anskaffelse og drift av IKT. Ifølge avdelingssjef ved CYFORs våpenskole, oberstløytnant Roger Johnsen, har CYFOR en funksjonell myndighet (intervju, 17.3.20). Forsvarets operative hovedkvarter er derimot tillagt operativ myndighet. Og på toppen av dette har Forsvarsmateriell fått delegert en teknisk myndighet. På papiret ser dette klart ut, ifølge Johnsen. Men i praksis flyter tekniske, funksjonelle og operative roller over i hverandre. Fra et brukerperspektiv på CYFORs våpenskole forklarer Johnsen at dette er fordi CYFOR ofte må omkonfigurere nettverk som Forsvarets operative hovedkvarter bruker, særlig i operasjoner mot dynamiske motstandere som hele tiden endrer sin *modus operandi*. Men også fordi de funksjonelle kravene som CYFOR setter til Forsvarets IKT-systemer får stor betydning for de tekniske løsningene som Forsvarsmateriell skal utarbeide. Dermed viskes grensene ut mellom de tre driftsenhetene (intervju, 17.3.20).

Måten Forsvaret tilnærmer seg en mer digitalisert hverdag på, selve «forretningsmodellen» til etaten, preges dermed av fundamentale svakheter. Dette erkjennes også av sjefen for CYFOR, generalmajor Inge Kampenes. Under Arendalsuka i 2019 hevdet han at Forsvaret «faktisk ikke er like flinke til å samarbeide [...] fordi vi har tillitsutfordringer, vi har maktkamper, vi prioriterer ikke eller tar oss ikke tid til å samarbeide, eller vi erkjenner ikke verdien i dette i en relativt fredelig hverdag» (Sævold, 2019). Den foregående CYFOR-sjefen opplevde akkurat det samme problemet. I 2017 valgte derfor generalmajor Odd Egil Pedersen å fratre stillingen fordi, som han selv sa det: «makt og myndighet ble pulverisert» (intervju, 18.3.20).

Denne problematikken er velkjent og godt dokumentert, blant annet av konsulentselskapet McKinsey & Co. I en rapport fra 2015 hevdet de at Forsvaret har valgt

> en uegnet organisering av IKT. Modellen bidrar til ansvarspulverisering og uløste oppgaver. Det er store uklarheter i ansvarsforhold og ingen unison begrepsbruk mellom funksjoner. Dette driver både duplisering av funksjoner, eksempelvis i skillet mellom forvaltning og drift, og uløste oppgaver, eksempelvis rundt brukerstyring av systemer. (2015, s. 51)

Konklusjonen finner også støtte i arbeidene til tidligere forsvarssjef Sverre Diesen (2005–2009). Etter nærmere 40 års tjeneste på alle nivåer i kommandokjeden konkluderte han med at Forsvaret i bunn og grunn var svært fragmentert (Diesen,

2011). På den ene siden vil sjefene for forsvarsgrenene og driftsenhetene være opptatt av å løse egne forsvarsoppgaver «på vegne av Konge og Fedreland», noe de også er pålagt fra regjeringens side. Men på den annen side må det også utvises lojalitet og samarbeidsevne internt i etatsledelsen. Også selv om dette kan føre til problemer i den driftsenheten man selv er sjef for. Det er dette, ifølge Diesen, som har gjort at sjefene for forsvarsgrenene har den vanskeligste jobben:

> I alle forsvarsgrener oppfattes [lederne] som forsvarsgrenens fremste tillitsmann. [De skal] kjempe for forsvarsgrens interesser overfor forsvarssjef og statsråd. Men samtidig også være forsvarssjefens nærmeste rådgivere i alle spørsmål som angår deres respektive forsvarsgrener, og medlemmer av et kollegium som skal og må ta et ansvar også for helheten. (Diesen, 2011, s. 241)

Digital umodenhet og manglende cyberberedskap kan dermed forstås som en konsekvens av hvordan forsvarsledelsen er satt sammen. Hver og en representerer lederne egne organisasjoner, med egne budsjettposter på statsbudsjettet, og med særegne forsvarsoppgaver i krise og krig. Dette gjør at forsvarsledelsen utsettes for et betydelig krysspress internt i egen organisasjon. Hvordan kommer dette krysspresset til uttrykk mer konkret? For å få en dypere forståelse av handlingslogikken kan to eksempler fra forvaltnings- og operasjonsmiljøene være nyttig.

Forvaltningsmiljøet

På forvaltningssiden var det mellom 2005 og 2017 vært sterk uenighet mellom de 14 driftsenhetene om hvordan IKT-systemer for personell, økonomi og logistikk skulle standardiseres. Ifølge seniorstabsoffiser i Forsvarsstabens Styringsavdeling, oberstløytnant Frode Berg, var hensikten med Forsvarets felles integrerte forvaltning (FIF) å gi etaten betydelige stordriftsfordeler og innsparingsmuligheter (intervju, 9.3.20). Ikke minst for et forsvar som, ifølge Berg, «brukte knappe ressurser på å opprettholde mer enn 460 ulike forvaltningssystemer for logistikk, lønn og HR» (intervju, 9.3.20). Å ta i bruk ny teknologi for å løse oppgavene på nye måter ville dessuten bidra til driftsbesparelser. Dette var viktig for å frigjøre penger til nye og mer fremtidsrettede investeringer (Bogen & Haakenstad, 2015, s. 166–178). Berg understreket imidlertid at innføringen av FIF møtte motstand. Skepsisen kom særlig fra Luftforsvaret, som opplevde at FIF ikke tok hensyn til de særegne kravspesifikasjonene som fulgte i kjølvannet av nye kampflyinnkjøp (intervju, 9.3.20). Det samme var tilfelle i Sjøforsvaret; forestående kjøp av nye fregatter ville kreve en annen type materiellkontroll og materiellforvaltning enn hva FIF la opp til (intervju, 9.3.20; Mobech-Hanssen, 2018, s. 21–23). Ifølge avdelingsdirektør i Forsvarsstabens planstab, Eigil Gulliksen, skjedde også innføringen av FIF utenfor etatens linjeorganisasjonen (intervju, 9.3.20), Nye mennesker og ny kunnskap ble rekruttert inn utenfra etatens egne rekker (intervju, 9.3.20). Selv om den mektige sjefen for Forsvarsstaben ledet den nyopprettede FIF-organisasjonen, var den interne motstanden sterk, ifølge Gulliksen. Forvaltningssystemets «alenegang» i implementeringsfasen bidro snarere til å

svekke den interne forankringen og eierskapet. Dette var særlig tilfellet i driftsenheter som, ifølge Berg og Gulliksen, var mer opptatt av hvordan egne våpensystemer skulle driftes og forvaltes (intervju med Berg og Gulliksen, 9.3.20).

Operasjonsmiljøet

Det digitale etterslepet har også beredskapsmessige konsekvenser, fordi organisatorisk fragmentering og fraværet av helhetlige løsninger øker sårbarheten i de militære styrkene. Lav digital modenhet har, ifølge Cyberutredningen, vært kjent i lang tid. Ifølge utvalget som skrev utredningen har de interne problemene i Forsvaret skapt «vesentlige mangler på alle nivåer» i kommandokjeden (Forsvaret, 2019, s. 7). Særlig vanskelig er det å få på plass et IKT-system som hensyntar de operative behovene til alt fra Hærens artillerienheter på Setermoen, til luftforsvarssystemer på Ørlandet, til Sjøforsvarets fregattsystemer i Bergen. Det praktiske uttrykket for dette er at digitaliseringen i Forsvaret lett kommer ut av kontroll. Dette skyldes i stor grad, ifølge professor Mass Soldal Lund ved Cyberingeniørskolen, at det er svært vanskelig – om ikke umulig – å utvikle standardiserte digitale løsninger til en etat som må drifte «sitt eget flyselskap, sitt eget rederi og sin egen kjøretøypark» med blant annet artilleri, stormpanservogner og stridsvogner (intervju, 16.3.20). Etter hvert som de operative enhetene knyttes sammen i nettverk rundt om i landet oppstår det derfor, ifølge professoren i informasjonssikkerhet, en uformell blanding av sentral styring fra toppen og en lokal tilpassing fra bunnen i kommandokjeden (intervju, 16.3.20).

CYFOR støtter blant annet de militære styrkenes digitale behov ved å overføre store mengder data (transmisjon) gjennom tre regionale kontorer i Sør-, Midt- og Nord-Norge. Men samtidig skjer det kontinuerlige lokale tilpassinger av datasystemer ute i de luft-, sjø- og landmilitære avdelingene. Dette er enheter som på døgnkontinuerlig basis løser oppdrag i Barentshavet, langs russergrensen i Finnmark og i tilstøtende luftrom utenfor kysten. Disse avdelingene trenger, ifølge Lund, raskt «å fikse problemene sine» (intervju, 16.3.20). Dette er dels fordi CYFOR selv har kapasitetsproblemer (Forsvaret, 2019), men det er også fordi IKT-systemene ute i felten tidvis oppleves som lite brukervennlige, noe som gjør at avdelingene velger «raske løsninger» eller «snarveier». Med dette menes improviserte måter å bruke IKT-systemene på. Dette gjør riktignok at oppdrag kan løses raskt og effektivt, hevder Lund, i tråd med forventningene fra Forsvarets operative hovedkvarter. Men i den digitale infrastrukturen skapes det samtidig store sårbarheter som det er lett for motparten å utnytte (intervju, 16.3.20).

En kulturell fortolkning

Så langt har vi brukt instrumentelle forklaringsmekanismer for å forstå det digitale etterslepet i Forsvaret. Spørsmålet er om det også er andre årsaksforhold som er virksomme? Det vil si forhold som oppstår lengre nede i organisasjonen, i kollegiale nettverk og praksisfellesskap der luft-, sjø- og landmilitære avdelinger utvikler

særegne måter å forstå verden på? For militære beredskapsorganisasjoner er den forsvarsgrenvise korpsånden som bygger på lojalitet, samhold og disiplin viktige suksesskriterier i møtet med fienden. Men sterk korpsånd kan også føre til unødig rigiditet og innadvendthet. Dette gjelder særlig når etablerte praksiser utfordres og tar oppmerksomheten vekk fra den tradisjonelle måten oppdragene har blitt løst på. Dette perspektivet føyer seg dermed inn i rekken av tidligere studier der kulturelle årsaksforhold blir brukt til å tolke og forstå Forsvarets operative praksis. Mistanken om at dette kan være tilfelle i vår analyse forsterkes av empirien som er innhentet gjennom intervjuer, dokumentanalyser og tidligere forskning.

Her fremkommer det blant annet at Forsvarssjefens føringer, slik disse ble formidlet til de respektive forsvarsgrenene i perioden 2013–2019, har hatt liten effekt. Etter seks år var det fremdeles bare et fåtall av de luft-, sjø- og landmilitære styrkene som opplevde at cyberoperasjoner var en integrert del av hverdagen (Forsvaret, 2019, s. 17; McKinsey & Co., 2015, s. 56). Mer enn 20 år etter at Forsvaret selv innførte et nettverksbasert forsvar (Forsvaret, 1999), var det snarere slik at militær trening og øving langt på vei ble knyttet til forsvarsgrenenes tradisjonelle oppdragsportefølje, med adskilte luft-, sjø- og landmilitære domener. Forsvar og egenbeskyttelse mot ondsinnede cyberangrep ble bare trent sporadisk. Det var også, ifølge Cyberutredningen, «liten til moderat aktivitet» når det gjaldt integrerte fellesoperative øvelser. Ifølge seksjonssjefen for Digitalisering og innovasjon i CYFORs planstab, kommandørkaptein Tom Kjetil Landgraf, er de ansatte ofte «dyrket frem i egen forsvarsgren, noe som bidrar til at fellesoperasjoner ofte anses som temmelig abstrakt i forhold til mer håndfaste luft-, sjø- og landoperasjoner. Dette så vi særlig når egne IKT-systemer skulle endres eller standardiseres» (intervju, 25.3.20). Til tross for at stadig mer nasjonal forsvarsevne ble digitalisert og knyttet opp til nettverk med sivile forgreninger, var viljen til å øve på cyberoperasjoner rundt om i det ganske land liten (intervju, 25.3.20). Denne bekymringen ble også delt av avdelingssjefen på CYFORs våpenskole. Ifølge oberstløytnant Roger Johnsen ble det ikke utviklet realistiske bilder av hvilke sårbarheter egen avdeling hadde; ei heller hvilke cybertrusler Forsvaret stod overfor mer allment. Dette skyldtes at de respektive styrkene i luft-, sjø- og landforsvaret i liten grad prioriterte cybersikkerhet, cyberoperasjoner og cyberberedskap (intervju, 17.3.20. Se også Forsvaret, 2019).

Til tross for spede forsøk fra forsvarsgrenene på å integrere cyberoperasjoner i trening og øving, var så vel Forsvarssjefen som sjef CYFOR og Cyberutvalget som skrev cyberutredningen bekymret: Forsvarets innsats er fragmentert og sporadisk, og mannskapene mangler nødvendig kompetanse. Kvaliteten på «cyber-spill under øvelsene er lav og problemstillinger håndteres på et svakt militærfaglig grunnlag» (ibid, s. 17). Dette ble også bekreftet fra Planstaben i CYFOR. Ifølge kommandørkaptein Tom Kjetil Landgraf hadde CYFOR «riktignok [...] ansvaret for å rulle ut det digitale nervesystemet, men de hadde ingen reell myndighet til å pålegge forsvarsgrenene hvordan det nye systemet skulle tilpasses og brukes sammen med sine egne løsninger» (intervju, 25.3.20). Den militære selvransakelsen kulminerte langt

på vei med foredraget til sjef CYFOR under den årlige talen i Oslo Militære Samfund i 2019. I sitt hovedinnlegg tok generalmajor Kampenes bladet fra munnen og hevdet at hele det norske forsvaret risikerte å stagnere og bli irrelevant. Dette er fordi sikkerheten til stat og samfunn i siste instans baserer seg på en fungerende digital infrastruktur (Kampenes, 2019).

Stiavhengigheten som knyttes til forsvarsgrenenes egne ønsker om å prioritere egne kjerneoppdrag har lite med instrumentell rivalisering og tautrekking å gjøre. Snarere kan det skyldes innarbeidet praksis med sterk forsvarsgrenvis forankring. Dette gjelder særlig i spørsmålet om hva som anses som viktigst, og hva som følgelig er mindre viktig. Slike vurderinger skjer ikke ut ifra helhetlige forsvarsperspektiver, men ut ifra hva som er forventet adferd i den luft-, sjø- eller landmilitære avdeling man selv lever og ånder for.

Operative eksempler

Denne vurderingen finner støtte i Cyberutredningen, der det ble hevdet at trening og øving på cyber ikke prioriteres nedover i kommandokjeden, rett og slett fordi denne formen for virksomhet «kommer i veien for andre øvingsmål» (Forsvaret, 2019, s. 7). Ifølge professor Mass Soldal Lund ved Cyberingeniørskolen skyldes dette at øving på beskyttelse mot cyberangrep innebærer mye ventetid. Dette gjelder især for de taktiske avdelingene som er så uheldige å bli rammet, fordi den digitale infrastrukturen som styrkene trenger for å løse oppdragene lammes (intervju, 16.3.20). Men dermed opplever også avdelingene ute i felt at verdifull tid og mye penger kastes bort. For når alle må sitte og vente, siden sambandssystemene ikke lenger virker, blir hver og en satt ut av spill (intervju, 16.3.20). Dette ble også understreket av den tidligere sjefen for CYFOR, generalmajor Odd Egil Pedersen: Øvelser som simulerer fiendtlige cyberangrep der kommando- og kontrollsystemer eller GPS-signaler forsvinner nedprioriteres til fordel for forsvarsgrenvise kjernefunksjoner som for eksempel manøver, samvirke, ild og bevegelse (intervju, 18.3.20). Dette skyldes, ifølge kommandørkaptein Landgraf fra CYFORs planstab, at «forsvarsgrenene bygger opp en særegen kultur rundt de kapasitetene man selv er helt avhengige av for å få løst forsvarsgrens kjerneoppgave. Men dette er bare en fortsettelse av det tradisjonelle plattformsentrerte forsvaret – med forsvarsgrenvise fly, kjøretøyer og fartøyer. Det er ikke nettverksbasert» (intervju, 25.3.20).

Svak cyberberedskap og manglende egenbeskyttelse kan dermed forstås som et introvert ønske om å bli enda bedre på det som er forsvarsgrenenes *raison d'être*: luft-, sjø- og landmilitære slag mot fiendtlige styrker som i all hovedsak er trent og utstyrt som en selv. Denne vurderingen sammenfaller med andre forsknings- og utredningsarbeider som er gjort av de forsvarsgrenvise kompetansemiljøene i Forsvaret. I en masteroppgave om operativ erfaringshåndtering i Forsvaret er det først og fremst «kulturelle normer og verdier, samt en selvdefinert passende adferd, [som styrer] hvordan erfaringshåndteringen praktiseres i Hæren, Luftforsvaret og Sjøforsvaret (Erstad & Folkestad, 2016). I en analyse av Forsvarets skolemiljøer ble det avdekket

at kompetansemiljøer i så vel Hæren som i Luft- og Sjøforsvaret handlet mer ut ifra selvoppholdelsesdrift og lokal korpsånd enn ut ifra overordnede strategiske forsvarshensyn. I denne såkalte «Dekanstudien» fra Forsvarets høgskole ble det sågar hevdet at «grendelte utdanningsinstitusjoner har utviklet seg […] i isolat fra de andre grenene», noe som har vært svært uheldig for «felles perspektiver, felles løsninger [og] faglige synergier» (Bjerga et al., 2016, s. 2). Dette kom blant annet til uttrykk i måten forsvarsgrenenes krigsskoler forberedte seg på før de selv skulle slås sammen til en felles høgskole. I forkant av sammenslåingen brukte blant annet Luftkrigsskolen i Trondheim innleide konsulenter fra private selskaper for «å tydeliggjøre egne behov» fordi det viktigste var «å lage en strategi for at særegenheter [i Luftforsvaret] ivaretas» (Carlsten, Skaug & Haugdal, 2016, s. 21).

Bristende forventning

Problemene med å tilpasse seg digitale trusler ser ut til å følge instrumentelle og kulturelle spor. Utfordringene står like fullt i kontrast til de politiske forventningene som stilles til etaten. Ifølge Solberg-I regjeringen skulle *hele* Forsvaret «være i stand til å iverksette forebyggende sikkerhetstiltak» og avdekke cyberangrep i egen digital infrastruktur (Forsvarsdepartementet, 2016, s. 19). Det ble også forventet at *hele* Forsvaret skulle «motstå angrep i og gjennom det digitale rom for å sikre egen handlefrihet», ikke minst fordi dette var «viktige elementer i et lands forsvar» (ibid., s. 35). Stortinget har imidlertid lagt merke til at CYFOR mer var å anse som en «organisasjon for IKT-virksomhet i Forsvaret», og ikke «et mer relevant virkemiddel for militære cyberoperasjoner» (Stortinget, 2016, s. 11). Dermed har det oppstått en forventningsbrist i synet på Forsvarets cyberberedskap: «Stortingets intensjon ved etableringen av Cyberforsvaret var å legge grunnlag for en *helhetlig* organisasjon for å forsvare samfunnet mot militære eller statlige cybertrusler» i krise og krig (Stortinget, 2016, s. 39; forfatternes utheving).

Konklusjon

I denne artikkelen har vi beskrevet Forsvarets digitale modenhet og tolket det digitale etterslepet med organisasjonsteoretiske briller. Hvilken konklusjon kan utledes?

Hovedkonklusjonen er at Forsvarets styringsmodell er uegnet for å gi norske myndigheter en troverdig cyberberedskap i de militæres egne rekker. Det norske forsvaret er dermed ikke selv i stand til å forsvare seg selv mot de mest presserende truslene som deres egen etterretningstjeneste og Politiets sikkerhetstjeneste advarer mot. Dette er et paradoks, og kan best forstås i lys av den fragmenterte styringsmodellen til etaten. Intern uenighet mellom generaler og ledere fra ulike driftsenheter snevrer inn Norges militære handlingsrom når det gjelder å forsvare Forsvaret mot de mest presserende utfordringene. Dermed kan Forsvaret selv ses på som en sikkerhetsrisiko. Dette er en original måte å forstå nasjonale sikkerhetsutfordringer

på. Men ved å anlegge dette perspektivet kan norske sikkerhetsutfordringer vel så mye rettes innover i egen organisasjon som utover mot andre land. I stedet for nokså ensidige risikovurderinger av potensielle motstandere i for eksempel Russland og Kina (Etterretningstjenesten, 2020; PST, 2020), kan det være vel så viktig å rette søkelyset mot feil og mangler i egen organisasjon.

Samtidig som resten av samfunnet gjennomgår en rivende digitalisering, kan det synes som at Forsvaret står fast i en organisatorisk hengemyr som gjør det vanskelig å oppfylle politiske forventninger. Det er riktig nok enkelte forhold som peker i riktig retning, noe blant annet oberstløytnant og seksjonssjef ved CYFORs våpenskole, Roger Johansen, understreket: Forsvaret har en internasjonalt ledende *Norwegian Battle Lab* med sterk innovasjonskraft langt utenfor Norges grenser (intervju, 17.3.20). Men evnen til å omsette nye ideer og nye arbeidsmåter til praktisk handling hjemme i Norge, i egen etat, viser seg dessverre å være svært vanskelig.

Om forfatterne

Tormod Heier er oberstløytnant i Hæren, forskningsleder ved Stabsskolen og professor i statsvitenskap ved Forsvarets høgskole. Heier har tidligere jobbet i Etterretningstjenesten, Forsvarsdepartementet og i Afghanistan, og har de senere år utgitt en rekke bøker og artikler om norsk og europeisk forsvars- og sikkerhetspolitikk i inn- og utland.

Bjørn E. Mobech-Hanssen er doktorgradskandidat ved Institutt for statsvitenskap, Universitetet i Oslo. Mobech-Hanssen er offiser og stipendiat ved Forsvarets høgskole, Stabsskolen, har militær utdannelse fra Krigsskolen og Forsvarets høgskole, samt hovedfag i statsvitenskap fra Universitetet i Tromsø.

Litteratur

Allison, G. T. & Zelikow, P. (1971). *Essence of decisions. Explaining the Cuban Missile Crisis*. Boston: Little Brown.

Bjerga, K. I., Skaug, R., Espevik, R., Haug, K. E., Pedersen, O. & Pedersen, T. (2016). *Dekanstudien 2016*. Oslo: Forsvarets høgskole.

Bogen, O. & Håkenstad, M. (2015). *Balansegang: Forsvarets omstilling etter den kalde krigen*. Oslo: Dreyers forlag.

Bouckaert, G., Peters, B. G. & Verhoest, K. (2010). *The coordination of public sector organizations: Shifting patterns of public management*. London: Palgrave Macmillan.

Carlsten, T. C., Skaug, R. & Haugdal, B. K. (2016). *Krigsskolens relevans?* (NIFU Arbeidsnotat 2016:6). Hentet fra https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/2397983/NIFUarbeidsnotat2016-6.pdf?sequence=1&isAllowed=y

Christensen, T. (2017). Strategisk kompetanseledelse som fenomen: mote eller ny substans? I T. Heier (Red.), *Kompetanseforvaltning i Forsvaret* (s. 52–68). Oslo: Universitetsforlaget.

Christensen, T., Egeberg, M., Lægreid, P., Roness, P. G. & Røvik, K. A. (2017). *Organisasjonsteori for offentlig sektor* (3. utg.). Oslo: Universitetsforlaget.

Colombo, M., Dagnio, G. B., Lehmann, E. E. & Salmador, M. (2019). The governance of entrepreneurial ecosystems. *Small Business Economics*, *52*(1), 419–428. https://doi.org/10.1007/s11187-017-9952-9

Cunningham, J. A., Menter, M. & Wirsching, K. (2019). Entrepreneurial ecosystem governance: A principal investigator-centered governance framework. *Small Business Economics*, *52*(1), 545–562. https://doi.org/10.1007/s11187-017-9959-2.

Diesen, S. (2011). *Fornyelse eller forvitring? Forsvaret mot 2020*. Oslo: Cappelen Damm.

Dutton, W. H., Creese, S., Schillair, R. & Bada, M. (2019). Cybersecurity capacity. Does it matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Eide, O. K. & Nørstebø, C. (2017). Vår evne til å stå imot et cyberangrep er marginal (Publisert 11. oktober 2017 10:58. Sist oppdatert 18. oktober 2017 09:10). *Forsvarets forum*. Hentet fra https://forsvaretsforum.no/v%C3%A5r-evne-til-%C3%A5-st%C3%A5-i-mot-et-cyberangrep-er-marginal

Elvenes, H., Sivertsen, E. & Skotåm, P.-G. (2019, 28. oktober). *Debatt om cybertrusselen mot Norge*. Innlegg fra konferansen Sikkerhetspolitisk balansekunst i regi av UTSYN, Bodø. Hentet fra https://www.facebook.com/highnorthnews/videos/2506680956093205/

Erstad, K. & Folkestad, E. (2016). *Operativ erfaringshåndtering i Forsvaret* (Masteroppgave, UiT Norges arktiske universitet). Hentet fra https://hdl.handle.net/10037/9415

Etterretningstjenesten. (2020). *Fokus 2020*. Hentet fra https://forsvaret.no/presse_/ForsvaretDocuments/Fokus2020-web.pdf

Eurostat. (2019). *Eurostat regional yearbook 2019 edition*. Hentet fra https://ec.europa.eu/eurostat/documents/3217494/10095393/KS-HA-19%E2%80%91001-EN-N.pdf/d434affa-99cd-4ebf-a3e3-6d4a5f10bb07

Flyverbom, M., Deibert, R. & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, *58*(1), 3–19. https://doi.org/10.1177/0007650317727540

Forsvaret. (2018). *Digitaliseringsstrategi for Forsvaret*. Oslo: Forsvarsstaben.

Forsvaret. (2019). *Forsvarssjefens fagmilitære råd, 2019 – rapport fra cyberutredningen*. Oslo: Forsvarsstaben.

Forsvaret. (2020). Forsvarets organisasjon. Hentet fra https://forsvaret.no/organisasjon

Forsvarsdepartementet. (2016). *Kampkraft og bærekraft — Langtidsplan for forsvarssektoren*. (Prop. 151 S (2015–2016)). Hentet fra https://www.regjeringen.no/no/dokumenter/prop.-151-s-20152016/id2504884/

Forsvarsdepartementet. (2018). *Proposisjon til Stortinget (forslag til stortingsvedtak)*. (Prop. 1 S (2018–2019)). Hentet fra https://www.regjeringen.no/contentassets/0d9a279e01a94aa395e95018718ab2b7/no/pdfs/prp201820190001_fddddpdfs.pdf.

Heier, T. (2018). Military samhandling – formal and informal behaviour in Norway's armed forces. I G.-E. Torgersen (Red.), *Interaction: 'Samhandling' under risk. A step ahead of the unforeseen*. (s. 301–318). Oslo: Cappelen Damm Akademisk.

Heier, T. (2019). *Et farligere Norge?* Bergen: Fagbokforlaget.

Jacobsen, D. I. (2010). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode* (2. utg.). Kristiansand: Høyskoleforlaget.

Jensen, M. S. (2019). Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer. *Internasjonal Politikk*, *77*(3), 266–277. https://doi.org/10.23865/intpol.v77.1369

Johnsen, R. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal politikk*, *71*(2), 241–251. Hentet fra https://www.idunn.no/ip/2013/02/cyberkrigfoering_og_forsvaretsoperative_evne

Kampenes, I. (2017, februar). *Operasjonalisering av beskyttelse mot en ny og fremvoksende trussel*. Tale i Oslo Militære Samfund, Oslo. Hentet fra https://oslomilsamfund.no/2017/02/20/foredrag-cyberforsvaret-operasjonalisering-av-beskyttelse-mot-en-ny-og-fremvoksende-trussel/

Kampenes, I. (2019, oktober). *Utviklingen av militær cybervirksomhet i lys av det fagmilitære råd*. Tale i Oslo Militære Samfund, Oslo. Hentet fra https://oslomilsamfund.no/2019/10/15/foredrag-sj-cyfor-generalmajor-inge-kampenes-utviklingen-av-militaer-cybervirksomhet-i-lys-av-det-fagmilitaere-rad/

Kristiansen, M. & Hoem, N. (2019). Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv. *Internasjonal Politikk*, *77*(3), 252–265. https://doi.org/10.23865/intpol.v77.1385

Kommunal- og moderniseringsdepartementet. (2018, 8 oktober). *Tidenes største satsing på digitalisering* [Pressemelding]. Hentet fra https://www.regjeringen.no/no/aktuelt/tidenes-storste-satsing-pa-digitalisering/id2614074/

March, J. G. & Olsen, J. P. (1989). *Rediscovering institutions. The organizational basics of politics*. New York: The Free Press.

McKinsey & Company. (2015). *Modernisering og effektivisering av stabs-, støtte- og forvaltningsfunksjoner i forsvarssektoren*. Hentet fra https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/150317modernisering-og-effektivisering-av-forsvarssektoren.pdf.

Mobech-Hanssen, B. E. (2018). *Forsvarets logistikkprosjekt. Halvparten levert, forsinket og til dobbel pris*. (Institutt for forsvarsstudier/IFS Insights 6/2018).

Moen, J. V. (2019, desember). *Presentasjon av Forsvarets digitaliseringsstrategi*. Foredrag på Forsvarets høgskole, Oslo.

Muller, L. P. (2019). Inn i gråsonen: avskrekking som forsvar av cyberspace?. *Internasjonal Politikk*, 77(3), 288–295. https://doi.org/10.23865/intpol.v77.1397

Olsen, J. P. (1988). *Statsstyre og institusjonsutforming*. Oslo: Universitetsforlaget.

Pedersen, O. E. (2015, februar). *Gir IKT-satsingen til Forsvaret en forsvarbar informasjonsinfrastruktur og et fundament for moderne militære operasjoner?* Tale i Oslo Militære Samfund, Oslo. Hentet fra https://oslomilsamfund.no/2015/02/02/foredrag-gir-ikt-satsingen-til-forsvaret-en-forsvarbar-informasjonsinfrastruktur-og-et-fundament-for-moderne-militaere-operasjoner/

Politiets sikkerhetstjeneste. (2020). *Nasjonal trusselvurdering 2020*. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Riksrevisjonen (2011). *Riksrevisjonens undersøkelse av intern kontroll i forsvarssektoren*. (Dokument 3:9 (2010–2011)). Hentet fra https://forsvaret.no/ifs/ForsvaretDocuments/Dokument%20nr.%203_9%20(2010–2011)%20Riksrevisjonen%20unders%C3%B8kelse%20av%20intern%20kontroll%20i%20forsvarssektoren.pdf.

Røgeberg, O. (2019). *Norge i europatoppen i bruk av offentlige nettjenester* (SSB rapport). Hentet fra https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/norge-i-europatoppen-i-bruk-av-offentlige-nettjenester

Røise, M. B. (2017). *Tirsdag samlet norske IT-toppledere seg for et viktig møte. Onsdag kveld stilte de en rekke krav til Erna Solberg*. Hentet fra https://www.digi.no/artikler/tirsdag-samlet-norske-it-toppledere-seg-for-et-viktig-mote-i-kveld-stiller-de-en-rekke-krav-til-erna-solberg/367461

Selznick, P. (1957). *Leadership in administration: A sociological interpretation*. New York: Harper & Row.

Smircich, L. (1985). Is the concept of culture a paradigm for understanding organizations and ourselves? I P. N. Frost, L. F. Moore, M. R. Louis, C. C. Lundberg & J. Martin (Red.), *Organizational culture* (s. 55–72). Thousand Oaks, CA: Sage.

Stortinget. (2016). Innst. 62 S (2016–2017). Innstilling til Stortinget fra utenriks- og forsvarskomiteen. Hentet fra https://stortinget.no/globalassets/pdf/innstillinger/stortinget/2016-2017/inns-201617-062s.pdf

Svenungsen, B. (2019). *Vårt digitale fundament*. (Institutt for forsvarsstudier/IFS Insights 5/2019).

Sævold, H. (2019, 15. august). Cyberforsvaret: – Vi må erkjenne at vi står oppi en ganske utfordrende situasjon. *Digi.no*. Hentet fra https://www.digi.no/artikler/cyberforsvaret-vi-ma-erkjenne-at-vi-star-oppi-en-ganske-utfordrende-situasjon/471572

Thompson, J. D. (2007). *Organizations in action. Social science bases of administrative theory* (5. utg.). Piscataway, NJ: Transaction Publishers.

Tømmerbakke, S. G. (2019, 4. november). Cyberforsvaret: Forsvarets lim og digitale rustning. *High North News*. Hentet fra https://www.highnorthnews.com/nb/cyberforsvaret-forsvarets-lim-og-digitale-rustning

Wareham, J., Fox, P. B. & Giner, J. L. C. (2014). Technology ecosystem governance. *Organization Science*, *25*(4). https://doi.org/10.1287/orsc.2014.0895

Westerman, G., Bonnet, D. & McAfee, A. (2014). *Leading digital: Turning technology into business transformation*. Boston, MA: Harvard Business Review Press.

Intervjuer

Berg, F. (2020, 9. mars). Intervju. Berg er oberstløytnant og stabsoffiser i Styringsavdelingen i Forsvarsstaben.

Gulliksen, E. (2020, 9. mars). Intervju. Gulliksen er avdelingsdirektør i Styringsavdelingen i Forsvarsstaben.

Landgraf, T. K. (2020, 25. mars). Telefonintervju. Landgraf er kommandørkaptein i Sjøforsvaret og seksjonssjef i Seksjon for digitalisering og innovasjon ved Planstaben i Cyberforsvaret (permisjon fra Forsvaret fra 2019).

Lund, M. S. (2020, 16. mars). Telefonintervju. Lund er professor i informasjonssikkerhet ved Cyberingeniørskolen ved Forsvarets høgskole.

Pedersen, O. E. (2020, 18. mars). Telefonintervju. Pedersen er generalmajor (P) og tidligere sjef for CYFOR.

Johnsen, R. (2020, 17. mars). Telefonintervju. Johnsen er oberstløytnant og sjef for Konsept- og strukturavdelingen ved Våpenskolen i Cyberforsvaret.

Abstract
National Defence in a Digital Crisis?

Even though the Norwegian authorities are world leaders in digitalization of public services, its armed forces are falling behind. In its essence, the problem lies in a management model with 14 different services striving for power and influence. This is particularly so when it comes to whom should have supreme authority as information and communication technology (ICT) systems are standardised across the force. How can we describe, explain and comprehend this digital complexity? Contemporary research does not provide clear answers, much due to over-emphasis on external cyberthreats. The question of why Norway's armed forces are incapable of providing a proper defence against cyberthreats therefore remains unanswered. By means of instrumental and cultural theories, we find grave deficiencies due to internal rivalry and organisational fragmentation.

Keywords: digitalisation • Norway's armed forces • digital maturity • cyber readiness