FFI-rapport 2013/03101

Strategisk kommunikasjon som redskap i krisehåndtering

Janne Merete Hagen og Henning André Søgaard

FFI Forsvarets forskningsinstitutt

Strategisk kommunikasjon som redskap i krisehåndtering

Janne Merete Hagen og Henning André Søgaard

Forsvarets forskningsinstitutt (FFI)

13. mars 2014

FFI-rapport 2013/03101

1207

P: ISBN 978-82-464-2360-9
E: ISBN 978-82-464-2361-6

Emneord

Strategisk kommunikasjon

Informasjonsoperasjoner

Cyberforsvar

Influence (påvirkning)

IKT

Godkjent av

Kjell Olav Nystuen	Prosjektleder
Anders Eggen	Avdelingssjef

Sammendrag

Denne rapporten er skrevet for FFI-prosjektet ”Militære informasjonsoperasjoner”, og konkluderer med at strategisk kommunikasjon (stratkom) kan være en vesentlig ressurs for Forsvaret i krisehåndtering. I gjennomføring av langtidsplanen Prop. 73 S ”Et forsvar for vår tid” fastslår norske myndigheter at de særlig vil ”styrke Forsvarets evne til å utgjøre en krigsforebyggende terskel gjennom å videreutvikle Forsvarets samlede kapabiliteter og betrakte militære evner i et helhetlig perspektiv, både nasjonalt og i en alliert kontekst” (FD 2012). FFI mener strategisk kommunikasjon vil kunne understøtte denne oppgaven i fredstid på samme måte som strategisk kommunikasjon har understøttet opprørsbekjempelse i internasjonale operasjoner. Dette forutsetter imidlertid en helhetlig tilnærming, spesielt en større bevissthet rundt og kunnskap om mulighetsrom og utfordringer.

For en småstat som Norge vil de reelle maktmidlene ved en krise heller være internasjonal rett, politisk og diplomatisk kreativitet og kløkt, og regional og internasjonal legitimitet, snarere enn tradisjonell militærmakt. I dette bildet vil strategisk kommunikasjon kunne gi betydelig merverdi også for Forsvaret, i fredstid så vel som i militære oppdrag. Nato benytter i stadig større grad strategisk kommunikasjon i sine operasjoner, og som medlemsland er Natos retningslinjer gjeldende også for Norge. Utnytting av stratkoms potensial krever ikke nødvendigvis flere ressurser i Forsvaret, men bedre utnyttelse og koordinering av de ressursene som allerede eksisterer. I tillegg vil nytenking rundt hva påvirkning innebærer i et mangfoldig og uoversiktlig digitalt informasjonssamfunn være svært viktig. Merverdi forutsetter uansett at strategisk kommunikasjon integreres systematisk i operasjonsplanlegging, noe som ikke er tilfelle i dag.

Rapporten identifiserer utvalgte hovedutfordringer og muligheter relatert til strategisk kommunikasjon. Den første er diskursen rundt hva påvirkning innebærer, en diskurs som ofte assosieres med politisk ladete begrep som propaganda. Det andre spørsmålet er; hvordan skal strategisk kommunikasjon håndteres i en global verden hvor et budskap kan nå verden i løpet av sekunder, og hvor målgrupper endrer eller flytter seg, og en informasjonskampanjes effekt derfor blir stadig vanskeligere å måle? Mot dette bakteppe mener vi solid strategisk kommunikasjon i 2014 forutsetter solide (digitale) analyseverktøy for å kunne gjøre kontinuerlige strategiske vurderinger av effekt. Den tredje utfordringen er knyttet til Forsvarets intellektuelle kapital og hvordan Forsvaret sikrer tilstrekkelig kompetente ressurser. Strategisk kommunikasjon som verktøy i krisehåndtering krever utdanning, trening og øvelser, som igjen kan bidra til å redusere eventuell turnover og sikre kontinuitet. Den fjerde hovedutfordringen er knyttet til organisering, og peker på hvordan en tydeligere formalisering av et tverrsektorielt samarbeid vil være en forutsetning for å lykkes med strategisk kommunikasjon.

FFIs arbeid har avdekket behov for mer forskning på ikke-kinetisk maktbruk og krisehåndtering i informasjonsdomenet, samt studier av hvordan strategisk kommunikasjon kan utvikles videre for å bidra til forbedring av den norske forsvarsevnen.

English summary

This report is written as part of the FFI project «Military Information Operations», and concludes that strategic communication can be a significant resource for the Norwegian Military Forces in crisis management.

The political ambition of the Norwegian Government is to strengthen the crisis management and war and conflict prevention capabilities of the Norwegian Military Forces. Strategic communication has proved to be an important contributor to counter insurgency missions in international operations. Strategic communication has the potential to play an equally important role in crisis management and war and conflict prevention. The globalized world opens up a wide range of new strategic communication opportunities and challenges.

In particular, for a small state like Norway, strategic communication can add value to military operations. NATO has for a long time utilized strategic communication in its operations worldwide. As a NATO-member, Norway is obliged to abide by Nato's policy on strategic communication, and it is therefore important that strategic communication is integrated into the military planning processes as well. To that end, and in order to succeed, the perspectives of what strategic communication entails in a globalized world, should be renewed. In a potential conflict, the real power might lie in our ability to utilize diplomacy, creativity, international justice and legitimacy, rather than traditional kinetic military power. Moreover, due to the complexity of the globalized world, a comprehensive approach is needed, including the use of a variety of means like diplomatic, information, economy and military.

FFI has identified a few challenges and opportunities related to strategic communication from a Norwegian perspective. The first challenge is connected to what the term "influence" entails in the area of strategic communication. In Norway, the term has rather negative connotations and is often associated with propaganda. Another challenge is propelled by globalization, where targets move quickly, information flows non-stop and the word spreads fast. To keep up with the pace of information flow, the use of digital tools and platforms are required. FFI has also identified the utility of digital tools to measure effect of information campaigns in military operations. Looking to the organizational aspects, we have identified two challenges; one is related to the sustainability and growth of intellectual capital in the area of strategic communication and the other is related to improved cross-governmental cooperation. In order to stimulate intellectual capital development, we recommend that military exercises integrate strategic communication to a greater extent than has been done thus far.

Finally, our report underscores a further need for research on military non-kinetic use of power and how strategic communication can improve crisis management and war and conflict prevention.

Innhold

Forord

Elektronisk kommunikasjon og automatisert og digital tjenesteproduksjon har endret rammene for krigføring og politisk påvirkning. I dag kan verdensopinionen og ulike målgrupper potensielt nås med et tastetrykk. Samtidig gir livestrømming, ”crowdsourcing” og analyse av Big data bedre forutsetninger enn noen gang tidligere for å skape et sammensatt situasjonsbilde. I tillegg er det digitale domenet i seg selv blitt et krigsteater hvor kampen «om sannheten» utkjempes på Twitter, som i Gaza, eller i mediene, som med Snowden-lekkasjene om norsk overvåking i Dagbladet og E-tjenestens tilsvar i etterkant. Og sist, men ikke minst, når digital infrastruktur og tjenesteproduksjon utsettes for angrep, vil dette i seg selv kunne påvirke befolkningens tilgang til informasjon, basisvarer og viktige tjenester.

Prosjektet ”Militære informasjonsoperasjoner” ved Forsvarets forskningsinstitutt (FFI) har blant annet sett nærmere på hva de nye rammebetingelsene kan bety for Forsvarets operasjoner, hjemme og ute. I dette arbeidet har vi identifisert strategisk kommunikasjon (stratkom) som et sentralt område. I motsetning til tradisjonell presse- og informasjonsvirksomhet, handler stratkom mer om hvordan ord og handlinger blir *oppfattet*, enn om *hva* som faktisk blir sagt og gjort eller hvilke kanaler som blir brukt. Sagt på en annen måte; strategisk kommunikasjon handler mer om ”strategi” enn ”kommunikasjon” og beskriver de analytiske prosessene bak tiltakene. Stratkom og informasjonsoperasjoner er forankret i Natos policy på militære informasjonsoperasjoner og Direktiv for kommunikasjon i Forsvarssektoren (Nato 2009a;Nato 2012). Stratkom på strategisk nivå favner bredt og *inkluderer*, i følge gjeldende definisjoner, militære informasjonsoperasjoner og informasjonsvirksomhet rettet mot egen befolkning, verdenspressen og allierte.

Basert på vår forskning drøfter denne rapporten *hvorfor* strategisk kommunikasjon er en viktig ressurs for Forsvaret i krisehåndtering, samt hvilke utfordringer og muligheter som ligger i strategisk kommunikasjon.

I løpet av prosjektet har vi vært i kontakt med eksperter både nasjonalt og internasjonalt, herunder fagmiljøer ved UK Defence Academy, det britiske Forsvarsdepartementet og det danske Forsvarsakademiet. Vi har også hatt et konstruktivt samarbeid med Forsvaret og Forsvarsdepartementet. Vi takker alle som har bidratt med informasjon i arbeidet med denne rapporten.

Kjeller, 13.03.2014

Janne M. Hagen og Henning A. Søgaard

1 Innledning

1.1 Bakgrunn

De siste to tiårene har globalisering og nedbygging av sikkerhetspolitiske blokker endret betingelsene for militær maktbruk. Samtidig har verdens bruk og avhengighet av avansert kommunikasjonsteknologi og digitale tjenester på en side endret trusselbildet og generert nye sårbarheter, og på den annen også gitt Forsvaret nye virkemidler. Mens militær maktbruk tidligere handlet primært om ledelse og organisering av kinetiske virkemidler, må nå et mye større virkemiddelapparat vurderes forut for militær maktbruk og krisehåndtering. Betydningen av ikke-kinetiske maktmidler, inkludert informasjon og nye digitale tjenester, vil øke betraktelig i årene framover, spesielt for småstater som Norge.

FFI har siden 2011, gjennom prosjektet "Militære informasjonsoperasjoner", sett nærmere på temaet informasjonsoperasjoner (IO). I praksis innebærer dette muligheten, gjennom endring, påvirkning og bruk av informasjon, informasjonssystemer og informasjonsprosesser, til å angripe og påvirke en eller flere motparter, beskytte egne styrker og beslutningstakere, samt informere og engasjere tredjeparter. Informasjonsoperasjoner innebærer også integrering av ulike typer virkemidler med forskjellige egenskaper for samlet å oppnå mer og bedre militær effekt eller sikkerhetspolitisk mål.

Det norske grunnsynet har vært at kapabiliteter som delvis eller samlet utgjorde informasjonsoperasjoner skulle være et supplement til tradisjonelle kinetiske militære kapabiliteter. På den bakgrunn hadde FFIs IO-prosjekt søkelys på utfordringer knyttet til ledelse av informasjonsoperasjoner på operasjonelt nivå. Men i løpet av prosjektets løp ble det avdekket at mange av utfordringene har sitt utspring på strategisk nivå, og er knyttet opp mot det nært beslektede temaet strategisk kommunikasjon. Denne rapporten oppsummerer hovedfunnene i dette arbeidet.

1.2 Formål

Rapportens formål er tredelt:

1. Å introdusere strategisk kommunikasjon som en ressurs for Forsvaret
2. Å drøfte betydningen av strategisk kommunikasjon for å øke effekten av Forsvarets operasjoner
3. Å diskutere utvalgte utfordringer og muligheter relatert til strategisk kommunikasjon i informasjonsdomenet

1.3 Rapportens oppbygging

Kapittel 2 presenterer teori og metode. Kapittelet introduserer arbeidsmetoden, viktige begreper og teori relatert til strategisk kommunikasjon, påvirkning og Knowledge Management. Med bakgrunn i empiri, blant annet fra prosjektet, bruker vi dette rammeverket for å diskutere Forsvarets utfordringer relatert til strategisk kommunikasjon og influence/påvirkning.

Kapittel 3 gir et innblikk i informasjonsdomenets kompleksitet, hvilke utfordringer og muligheter som eksisterer for bruk av ikke-kinetiske virkemidler som informasjonsoperasjoner, strategisk kommunikasjon og annen militær informasjonsvirksomhet. Kapitlet gir også et kort sammendrag av sivilsamfunnets sårbarhet og mulig behov for militær bistand. Med dette som utgangspunkt blir utfordringer og muligheter relatert til strategisk kommunikasjon for forsvarssektoren drøftet.

Kapittel 4 setter søkelys på noen utfordringer knyttet til strategisk kommunikasjon på strategisk nivå i Forsvaret. Deretter ser vi nærmere på mulighetsrommet som en tettere integrering av strategisk kommunikasjon i stridshjulet åpner opp, også i vanlig fredsdrift.

Kapittel 5 oppsummerer hovedfunn og gir anbefalinger med hensyn til videre forskning.

2 Teori og metode

2.1 Arbeidsmetode

I arbeidet med denne rapporten har vi brukt en utforskende metode. Det innebærer at vi stiller åpne spørsmål for å finne ut mest mulig om et gitt tema. I denne sammenheng er temaet strategisk kommunikasjon for Forsvaret og krisehåndtering på strategisk nivå i informasjonsdomenet.

Det empiriske grunnlaget for denne rapporten er en workshop med Forsvarets sentrale kommunikasjonsvirksomhet, gjennomført i Situasjonssenteret (SITSEN) i Forsvarsdepartementet 5. desember 2012. Bakteppet var et scenario med informasjonskrigføring og militære informasjonsoperasjoner rettet mot Norge. Workshopen var basert på et scenario utviklet av prosjektet for en workshop ved Forsvarets operative hovedkvarter (FOH) samme år. Diskusjonene var strukturert rundt fire akter og ulike stadier i opptrappingen av krisen. I tillegg bygger rapporten på samtaler med ansatte og eksperter i Forsvaret, og møter med eksperter på informasjonsoperasjoner og strategisk kommunikasjon i Storbritannia og i Danmark.

Rapporten er videre basert på skriftlige kilder. Vi har søkt bredt etter relevant litteratur i FFIs biblioteksdatabase, i Natos databaser og i Forsvarets biblioteker/krigsskolene, samt på internettet. Sosiale medier som Facebook og Twitter er også benyttet i underlagsarbeidet. Dette har vi gjort fordi omfanget av litteratur om denne tematikken er omfattende, og fordi kvalitet, pålitelighet og objektivitet på ulike kilder varierer sterkt. For eksempel vil rapporter, aviser, blogger og andre ytringer relatert til konflikt og krig ofte være politisk farget og sjelden gi et objektivt bilde. Også media kan bli offer for propaganda. Bagdikian er inne på dette når han, med referanse til

situasjonen i USA, påpeker at pressen ofte henter informasjon fra personer i framskutte posisjoner. Holdninger og meninger til slike personer er viktige, men de formidler ikke alltid alle sider av historien. Dessuten er mediene dominert av få store aktører med sterke egeninteresser (Bagdikian 2004). I tillegg har mediene en hang til å foretrekke krisene framfor suksesshistoriene, jamfør Natos medieerfaringer fra Balkan-krigene (Siegel 1998). Derfor har vår måte å håndtere dette på vært, så langt det har latt seg gjøre, å bruke ulike kilder, med ulike innfallsvinkler. Kilder på internettet - inkludert avisartikler - er gjengitt i fotnoter, mens rapporter, vitenskapelige artikler og bøker er lagt inn som en egen referanseliste helt til slutt.

Avslutningsvis bygger rapportens konklusjoner på drøftinger av empirien innenfor et teoretisk rammeverk. Det teoretiske rammeverket gir viktige definisjoner, innføring i strategisk kommunikasjon, påvirkning (influence), medienes rolle, intellektuell kapital og Knowledge Management. Dette er viktige faktorer å ta med i drøftingene om strategisk kommunikasjon.

2.2 Viktige begreper og definisjoner

Det eksisterer en rekke definisjoner av **informasjonsoperasjoner (IO).** St.prp. nr. 48 (2007-2008) ”Et forsvar til vern om Norges sikkerhet, interesser og verdier” (kap 5.6.8) opererer med følgende fortolkning: ”Militære informasjonsoperasjoner er ikke en kapasitet i seg selv, men en strategi for å koordinere militære aktiviteter på informasjonsområdet” (Forsvarsdepartementet 2012b). Natos definisjon, som også er gjeldende for medlemslandet Norge, fastslår at “Info Ops is a staff function to analyze, plan, assess and integrate Information Activities (IA) to create desired effects on the will, understanding and capability of adversaries, potential adversaries and North Atlantic Council (NAC) approved audiences in support of Alliance mission objectives” (Nato 2012).

Informasjonsoperasjoner og strategisk kommunikasjon er videre forankret i Natos policy på militære informasjonsoperasjoner og direktiv for strategisk kommunikasjon (Nato 2009a;Nato 2012). Nato definerer strategisk kommunikasjon (stratkom) som “the coordinated and appropriate use of Nato communications activities and capabilities – Public Diplomacy, Public Affairs (PA), Military Public Affairs, Information Operations and Psychological Operations, as appropriate – in support of alliance policies, operations and activities, in order to advance Nato’s aims” (Nato 2009a).

Direktiv for Kommunikasjonsvirksomhet i Forsvarssektoren, som trådte i kraft 17. april 2013, tilsier at strategisk kommunikasjon er å forstå som ”den samlede innsats av tiltak rettet mot målgrupper for å nå spesifikke strategiske mål eller politiske målsettinger, og spenner fra politisk nivå og helt ut i organisasjonens utøvende ledd”[1]. Stratkom på strategisk nivå favner altså bredere, og *inkluderer* militære informasjonsoperasjoner og informasjon til egen befolkning, verdenspressen og allierte.

[1] Direktiv for kommunikasjonsvirksomhet, Kapittel 4, Forsvarsdepartementet 2013.

Militære informasjonsoperasjoner kan innbefatte bruk av flere virkemidler, både kinetiske og ikke-kinetiske. Disse inkluderer psykologiske operasjoner (psyops), elektronisk krigføring (EK), Computer Network Operations (CNO), Information Security (INFOSEC), fysisk ødeleggelse, Operations Security (OPSEC) og villedning. For en mer utfyllende forklaring og definisjoner av disse begrepene, se (Nato 2009b).

Informasjonsmiljøet defineres, i Natos gjeldende policy for informasjonsoperasjoner, som følger: ”The Information Environment (IE) comprises the information itself, the individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occur.” (Nato 2012) .

Videre heter det at ”…the importance of worldwide distributed information, the speed at which information is communication, the role of social media and the reliability of information systems have created a situation in which no Alliance decision or action can be taken without considering its potential impact on the IE.”

Cyberdomenet er definert som et globalt domene realisert gjennom fysiske eller logiske sammenkoplinger av informasjonssystemer. Dette inkluderer fysiske og virtuelle nettverksenheter, kommunikasjonsinfrastruktur, media og data (Windvik et al. 2013).

2.3 Strategisk kommunikasjon i militære operasjoner

I følge gjeldende definisjoner, det være seg Natos forståelse eller den norske forståelsen, er strategisk kommunikasjon et redskap som kan brukes til å understøtte oppnåelsen av langsiktige politiske mål. Strategisk kommunikasjon er derfor også mer strategi enn ren kommunikasjon, der strategien beskriver hvordan det, ved hjelp av ulike virkemidler, er mulig å nå et mål eller en ønsket sluttilstand (MoD 2012).

I militære operasjoner kommuniserer ofte handlinger sterkere enn ord (Nato 2010). Innenfor det sikkerhetspolitiske området er det en rekke virkemidler stater kan benytte som ledd i sitt arbeid for å påvirke. De siste årene har bruk av ”soft power” blitt stadig mer sentralt i ulike Nato-lands forsvar. I følge én forklaringsmodell, kan virkemidler innenfor denne kategorien deles inn i fire typer: diplomati, informasjon, militære og økonomiske, også forkortet på engelsk DIME. Bruk av disse virkemidlene kan gi effekt på følgende områder: politisk, militært, økonomisk, sosialt, informasjon og infrastruktur, forkortet (på engelsk) PMESII. IO og tilhørende pakke med virkemidler, jfr. kapittel 2.2, utgjør en delmengde av alle virkemidler som kan tas i bruk.

Mennesket har behov for å sette seg selv i en større sammenheng. Kultur, religion, tradisjon og normer former vår oppfatning av verden. Hendelser vi opplever forstås innenfor disse rammene. Mennesker med ulike oppfatninger, men innenfor samme målgruppe, vil derfor ha ulik fortolkning av en hendelse som inntreffer. Det speiler en utfordring i forhold til strategisk kommunikasjon, som forsøker å skape en definert oppfatning hos en eller flere målgrupper. I dette spiller *narrativet* en helt sentral rolle. Et narrativ er et system av historier som deler felles tema, former, hendelser og deltakere. Narrativet skaper forventninger for hvordan disse

elementene i kombinasjon kan dekke behov som har sitt opphav i krisen (Nissen 2011)[2]. På denne måten bør strategisk kommunikasjon bygge opp under sin egen historie, hvor narrativet er helt sentralt, og så prøve å endre målgruppenes oppfatning (persepsjon) slik at ønsket effekt oppnås (Bøe-Hansen 2013).

Strategisk kommunikasjon må ikke forveksles med propaganda, som utelukkende dreier seg om bruk av ord. Tatham omtaler strategisk kommunikasjon i militær sammenheng som en samordning av kommunikasjonseffekten av **alle** tiltak i en helhetlig kampanje, hvor ord og handling skal støtte opp under hverandre (Tatham 2008). Målet er helhetsinntrykket eller persepsjonen en avsender definerer som ønsket blant målgruppene. Dette skal i sin tur bidra til handlinger, som igjen skal bedre effekten av den militære operasjonen og til å oppnå det sikkerhetspolitisk ønskete sluttresultatet.

Paul et al (2010) har sett nærmere på et trettitalls konflikter i verden hvor militære ressurser har blitt satt inn for å bekjempe opprør. Forskerne fant blant annet at strategisk kommunikasjon har vært et sentralt og viktig virkemiddel for å lykkes med opprørsbekjempelse. Samtidig har strategisk kommunikasjon ofte ikke vært benyttet der de militære operasjonene har mislyktes (Paul et al. 2010). Grandhagen (Grandhagen 2011) påpeker at slike målinger av stratkom-effekt kan være en utfordring på grunn av manglende kvantitative data. Det er riktignok foretatt noen evalueringer av militære informasjonsoperasjoner og psykologiske operasjoner (Munoz 2013;Ward 2003). Men som vi skal komme tilbake til, er det mer utfordrende å måle effekten av ikke-kinetisk militærmakt sammenliknet med tradisjonell kinetisk militærmakt, både i forkant av og etter en operasjon. Det stiller spesielt strenge krav til metodikk og analyse.

2.4 Påvirkning i en globalisert verden

Det finnes en rekke ulike forklaringsmodeller for hvorfor folk lar seg påvirke til å endre holdning og atferd. Manheim (Manheim 2012) referer blant annet til Fishbein (1960), som baserer sin forklaring på individets tro, mens Festinger (1957), på sin side, utviklet dissonansteorien om menneskets trang til å være lik andre. Teorien om sosial bedømming hevder at endring oppnås hvis ny informasjon er tilstrekkelig lik til at den ikke føles truende. En annen forklaringsmodell er at påvirkning lykkes ut fra grad av opprinnelig engasjement og involvering hos målgruppen.

I følge Mc Fate er det omgivelsene som definerer rammene for hvilke typer kommunikasjon og virkemidler som bør brukes for å oppnå effekt. Å feildefinere omgivelsene kan gi den militære kampanjen et uheldig utilsiktet utfall (Mc Fate 2005). I en global verden er det også et faktum at én utvalgt målgruppe sjelden er budskapets eneste mottaker. Og når budskapet når mange, vil mottakerne ha ulike fortolkninger. Dette vil igjen ha utilsiktete effekter så vel på individer som på sosiale systemer (Larson et al. 2009).

Strategisk kommunikasjon vil derfor ikke bare kunne påvirke nasjonale aktører hvis disse er målgruppen, men, i en global verden, også internasjonale aktører. Hvorfor det er slik, kan også

[2] Se side 16.

forstås gjennom Thomas Hylland Eriksens dimensjoner for globalisering (Hylland Eriksen 2007). Dimensjonene kan, etter vårt syn, også gi rammer for å forstå strategisk kommunikasjon og internasjonal påvirkning, både når det gjelder målutvelgelse, valg av egnete virkemidler og analyse av effekt. I følge Hylland Eriksen kjennetegnes den globale verden av:

- Åpenhet, der for eksempel trusler fra internasjonal terrorisme kan ramme hvor som helst. Dette i kontrast til nasjonalstaten som den tradisjonelle trusselaktøren.
- Akselerasjon, der tid og rom blir komprimert, og nyheter sprer seg i løpet av sekunder
- Globale standarder, eksemplifisert ved verdensomspennende systemer som pengesystemet og datateknologi
- Konnektivitet, hvor de fleste kan nås gjennom tilknytning til internettet; det er oppunder 1 milliard domenenavn i 2013[3]
- Bevegelser og utbedt migrasjon. Av den grunn kan målgrupper forflytte seg og lokalisere seg på nye steder
- Miksing, der det finnes ulike modeller for sammenblanding av folk og kulturer, og målgruppene i konfliktområdet blir blandet
- Sårbarhet i forhold til hvordan befolkningen oppfatter risiko versus den reelle risikoen; det kan være store sprik mellom disse to
- Innebygging, der dette fungerer som en motkraft til globaliseringen gjennom å beskytte naturbefolkningen eller la egen identitet, tillit og sikkerhet knyttes til det nære og til lokalmiljøet

2.5 Tradisjonelle og sosiale medier - «digital dugnad»

Mediene har stor betydning for militære operasjoner, både som ressurs og som utfordrer. Den såkalte ”CNN-effekten” (Livingston 1997) antyder at medienes dekning kan bidra til å akselerere beslutningsprosesser, sette dagsorden og å påvirke operasjonssikkerheten. Den vil også kunne bidra til å endre folks holdninger, som igjen vil kunne påvirke politikken (Richter 2009). Erfaringer fra internasjonale operasjoner viser imidlertid at det kan være en utfordring å selge inn positive historier til media. Og når media heller skriver om terroristene, kan det raskt undergrave koalisjonens interesser og den politiske støtten i folket (Hubbard 2007). Et virkemiddel for å styrke interessen hos media har vært såkalt «embedded journalism», altså at journalister får mulighet til å følge med de militære styrkene ut på slagmarken. Denne metoden har vært hyppig brukt av både USA og av Nato, og kan være et effektivt virkemiddel for å spre et narrativ samt å signalisere åpenhet på kort sikt. Men dette kan også by på utfordringer for troverdigheten dersom journalisten eller leserne oppfatter et sprik mellom narrativet og virkeligheten på bakken (Haugen 2011).

Selv om tradisjonelle nyhetsmedier fremdeles utgjør en betydelig maktfaktor i påvirkning, utfordres disse nå i stadig større grad av mer åpne plattformer som mobiltelefon, internettet, digitale tjenester og sosiale medier. Sosiale medier gir bedre mulighet for raskere publisering over hele verden, en mer aktiv og interaktiv dialog med målgrupper og kan også bidra til en mer

[3] Internet Systems Concortium, www.ics.org/services/survey/, nedlastet 29.11.2013.

direkte og fortløpende rapportering fra slagmarken. Slik kan det offisielle narrativet gitt av stridende parter hele tiden bli justert og korrigert, mens en hel verden enten følger med, eller selv deltar.

Innovasjon av digitale tjenester bidrar også konstruktivt innen humanitært hjelpearbeid, og har gjort det mulig for befolkningen i rammede områder selv å bidra til et mer utfyllende situasjonsbilde. Dermed blir dette i seg selv også en maktfaktor å ta hensyn til i militære operasjoner - og dermed også i planlegging av strategisk kommunikasjon. I følge en rapport fra Harvard Humanitarian Initiative[4] er det fire hovedverktøy som benyttes til innsamling av informasjon og kommunikasjon med berørte miljøer: Høsting av data direkte fra folket (crowdsourcing), dataanalyse (Big data), krisekartlegging (crisis mapping) og digital datainnsamling (digital data collection) - inkludert validering av informasjon. Det er etablert flere internasjonale nettverk som bistår det formelle beredskapsapparatet med ulike tjenester. En paraplyorganisasjon er etablert for digitale hjelpere, Digital Humanitarian Network[5], hvor målet er å kople humanitære organisasjoner og kompetente frivillige tekniske miljøer.

Andre frivillige prosjekter og organisasjoner jobber mer med informasjonsstyring og støtter etablering av webbaserte krisestøtteverktøy og situasjonskart som integrerer informasjon til beredskapsaktører fra ulike kilder. Et eksempel er kommunikasjons- og informasjonsdelingsplattformen Ushahedi som ble skapt i forbindelse med urolighetene i Kenya i 2007. Ushahedi plattformen[6] kan fritt lastes ned fra internettet og gir mulighet for å bygge et bedre situasjonsbilde. Dette skjer gjennom frivillig digital rapportering via SMS; e-post, Twitter, etc inn i en nettbasert kartløsning. Gjennom slike tjenester kan folk flest bidra til å skape et mer komplett situasjonsbilde. I neste instans kan også myndighetene bruke slike redskap for å avsjekke egen situasjonsforståelse mot ”virkeligheten” der ute og samtidig få bidrag inn i effektvurdering av sine tiltak.

Det finnes dessuten stadig fler effektive verktøy for å overvåke digital aktivitet. Google Analytics gjør det for eksempel mulig å følge opp egne reklamekampanjer og hvordan målgruppen besøker eller bruker de digitale tjenestene (eksempelvis nettsider eller mobilapper) som blir tilbudt online.[7] Et eksempel på konstruktiv proaktiv bruk av slike tjenester er US Geological Services (USGS) sin bruk av mikrobloggetjenesten Twitter for varsling av jordskjelv, Twitter Earthquake Dispatch[8]. Tjenesten overvåker twittervarslinger om jordskjelv på ulike språk og fanger opp og videreformidler disse raskere enn tradisjonelle seismologiske instrumenter og tilhørende rutiner. Dermed kan varsling fra USGS nå hurtigere ut til målgruppene, og på den måten redde liv.

[4] Harvard Humanitarian Initiative. Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies. Washington, D.C. and Berkshire, UK: UN, Foundation & Vodafone Foundation Technology Partnership, 2011, http://www.unfoundation.org/assets/pdf/disaster-relief-20-the.pdf , nedlastet 28.10.2013.
[5] Se DH Network, homepage, http://digitalhumanitarians.com/ nedlastet 29.20.2013
[6] Se the Ushahedi platform, http://www.ushahidi.com/products/ushahidi-platform, nedlastet 29.20.2013.
[7] Google Analytics, http://google.com/analytics, nedlastet 23.12.2013.
[8] Tweet Earthquake Dispatch, USGS, http://earhquake.usgs.gov/ted/, nedlastet 23.12.2013.

På hjemlige trakter illustrerer terrorhandlingene 22. juli 2011 betydningen av media og strategisk kommunikasjon - både i forkant, i akuttfasen og i etterarbeidsfasen av en krise. Allerede to minutter etter bombeeksplosjonen klokka 15.25 avbrøt P4 sitt program "Midt i trafikken" med en ekstra nyhetssending. Kl. 15.42 rapporterte NRK P1s program "Her og Nå" om hendelsen, og norske og internasjonale TV-kanaler kastet om på sine sendeskjemaer for å dekke nyheten[9].

En lærdom fra 22. juli var at påtrykket fra media kommer umiddelbart, og at en beredskap for raskt å kunne bidra med korrekt informasjon til journalister og befolkning er helt avgjørende. Den dagen maktet verken systemer eller rutiner å håndtere presset. Dermed oppstod et vakuum med et enormt tilfang av vitner og egenobservasjoner, men der "…man ikke fikk den nødvendige kontakten med politiet for bekreftelser/avkreftelser. Resultatet var at rykter og spekulasjoner fikk florere, inkludert spekulasjoner om at Al-Qaida stod bak" (Time 2012). Evalueringen av politiets mediehåndtering avslørte også at media selv hadde store vansker med å få ut informasjon de første timene. De fleste opplysningene kom fra reportere på stedet, vitneobservasjoner og andre medier. Journalister mener at politiets informasjons- og mediehåndtering fungerte greit *etter* at Oslo-politiet hadde satt stab, men at innholdet ikke var på plass. Politiet var for tilbakeholdne og informasjon kom for sent, ble det fastslått. Geelmuyden Kiese har derfor i etterkant blant annet anbefalt at politiet i større kriser bør ha egen medieansvarlig på åstedet (Time 2012).

Politiets kommunikasjonsstrategi 22. juli er en interessant kontrast til måten de israelske styrkenes (IDF) vektla bruk av Twitter og YouTube i forbindelse med Israel-Gaza krigen i november 2012. For mens det norske politiet vektla kvalitetssikring og verifisering av all informasjon til allmennheten, var IDF opptatt av å publisere nyheter fortløpende, vel vitende om at informasjonsinnholdet ikke holdt et gjennomgående høyt presisjonsnivå. 14. november 2012 erklærte Israel krig mot Hamas. Det skjedde, trolig for første gang i historien, på mikrobloggtjenesten Twitter. Ledere på begge sider fortsatte å oppdatere sine statuser gjennom nyheter og trusler etter det første militære angrepet, og det ble også en arena hvor folk i Gaza kunne spre informasjon og desinformasjon[10]. IDFs talskvinne Avital Leibovich var helt åpen på at Twitter var bra for rask publisering uten redaksjonell kontroll, selv om det kunne resultere i at feilaktig informasjon kom ut. Som ledd i de digitale strategiske kommunikasjonsstrategiene har både IDF og Israels Ministry of Public Affairs etablert interaktive mediesentre, eller virtuelle situasjonsrom, hvor det samarbeides med bloggere og frivillige for å få meldinger ut [11]. I forkant av angrepet delte Israel ut flygeblader i Gaza der de oppfordret befolkningen til å holde seg borte

[9] Omtrent på samme tid (dvs. kvart på fire) var både administrativ og politisk ledelse av Justisdepartementet varslet.

[10] Battleground Twitter, Al Jazzera, 16. November 2012, http://stream.aljazeera.com/story/battleground-twitter-0022405 nedlastet 15 november 2012.

[11] Israel and Hamas wage social media fight via social media platforms, By Associated Press, Nov 16, 2012 02:00 AM EST
AP Friday, November 16, 3:00 AM, http://www.washingtonpost.com/business/israel-and-hamas-wage-social-media-fight-via-social-media-platforms/2012/11/15/637a5ff0-2f91-11e2-af17-67abba0676e2_story_2.html, nedlastet 16. November 2012.

fra Hamas og andre terrororganisasjoner [12]. Hamas, på sin side, har en egen flerspråklig webside de oppdaterer kontinuerlig, og kommuniserer med omverdenen via Facebook og SMS-lister. Dette viser hvordan partene i konflikter i stadig større grad tar i bruk nye digitale tjenester for å påvirke verdens støtte og utfallet av konflikten. Det spenner også ut et helt nytt mulighetsrom for villedning og propaganda.

Hvem eier så historien? Er det "førstemann ut"? Bøe-Hansen argumenterer for at Forsvaret bør komme så tidlig inn i nyhetsbildet som mulig når noe dramatisk er i ferd med å skje. Dette for å "ta kontroll" over budskapet og forhindre at nyhetsmedier, grunnet mangel på informasjon, blåser hendelsen ut av sine proporsjoner (Bøe-Hansen 2010). Men selv om dagens informasjonskappløp stiller krav til kjapp formidling, er det vel så viktig, ikke minst med tanke på Forsvarets troverdighet og tillit i befolkningen, å videreformidle korrekt informasjon. Høsten 2013 kunne Dagbladet "avsløre", takket være dokumenter lekket via NSA-avhopperen Edward Snowden, at 33 millioner mobilsamtaler i løpet av en måned var blitt overvåket. E-tjenesten reagerte raskt med å tilbakevise påstandene på en pressekonferanse og presiserte at den såkalte "overvåkingen" var koplet til militære operasjoner i utlandet. Det raske dementiet forhindret trolig at inntrykket om overvåking av egne borgere festet seg i Norge. Men selv ikke den raske responsen kunne forhindre at den opprinnelige versjonen av historien allerede hadde spredt seg kloden rundt via sosiale medier og internettet[13]. Hvem som egentlig vant informasjonskampen den dagen er dermed fortsatt et åpent spørsmål.

2.6 Kunnskapsdeling og organisasjonslæring

I rapporten "Strategic Influence Operation – the Information Connection" drøfter Brad M. Ward (U.S. Army College) hvordan informasjonssamfunnet har dimensjonert amerikansk krigføring fra 1. verdenskrig fram til terrorangrepet 11. september 2001. Et hovedfunn er at USAs tilnærming til informasjons- og influensoperasjoner hadde "alvorlige mangler" med hensyn til sentralisert koordinering og et funksjonelt tverrdepartementalt lederskap i informasjonsdomenet. Myndighetene hadde heller ikke maktet å utnytte potensialet i ny teknologi på tvers av ulike ansvarsområder, konkluderte Ward (Ward 2003).

Er så disse forutsetningene til stede i Norge? Svaret er både ja og nei (Hagen and Strand 2013). Norsk beredskap bygger på ansvar-, nærhets-, likhets- og etter 22. juli 2011, også samvirkeprinsippet. I totalforsvarskonseptet er det flere koordineringsgrupper og fora som skal bidra til at informasjon deles på tvers, at det eksisterer en felles situasjonsforståelse og at det jobbes mot felles mål. Et eksempel er Kriserådet, som består av sentrale embetsmenn, og er

[12] Three Israelis killed by rocket fired from Gaza Strip; Israel intensifies air offensive, By Karin Brulliard and Joel Greenberg,
Nov 15, 2012 11:22 AM EST, The Washington Post Published: November 14 | Updated: Thursday, November 15, 12:22 PM, http://www.washingtonpost.com/world/middle_east/hamas-leader-in-gaza-killed-by-israeli-strike/2012/11/14/de2ea690-2e72-11e2-9ac2-1c61452669c3_story.html, nedlastet 16. November 2012.

[13] Norway denies NSA collaboration – but admits to snooping on phone calls, Associated Press osl Oslo,19 November 2013, http://www.the guardian.com/world/2013/nov/19/norway-nsa-snooping-on-phone-calls, nedlastet 16.01.2014.

regjeringens viktigste organ under nasjonale kriser. Krisestøtteenheten (KSE), som er organisatorisk plassert i Justisdepartementet, er et permanent sekretariat for Kriserådet, og er også ment å være en ressurs som kan understøtte det som til enhver tid er lederdepartement med rådgiving og faglig bistand. Det innebærer at dersom Forsvarsdepartementet er lederdepartement, så vil Forsvarsdepartementet kunne trekke på ressurser fra KSE.

Men i en krisesituasjon hvor tiden er knapp, usikkerheten stor og det er mangel på validert informasjon, er det usikkert hvordan den norske modellen for krisehåndtering faktisk vil fungere. Norge har en offensiv tilnærming til teknologi og en uttalt ambisjon om digitalisering av forvaltningen. Samtidig er befolkningen høyt utdannet og nye generasjoner er fødte brukere av digitale verktøy. Det er likevel tvilsomt om potensialet som ligger i dette høye kompetansenivået er utnyttet fullt ut. La oss derfor se nærmere på hva kunnskap betyr. Studier har demonstrert at intellektuell kapital er positivt korrelert med organisasjoners verdiskapning (Cabrita and Vaz 2006). Vi mener dette også er gjeldende for militære organisasjoner som prioriterer dette i etterretningsarbeidet, samt i planlegging og gjennomføring av militære operasjoner. Dette leder oss inn på teorier om intellektuell kapital og Knowledge Management.

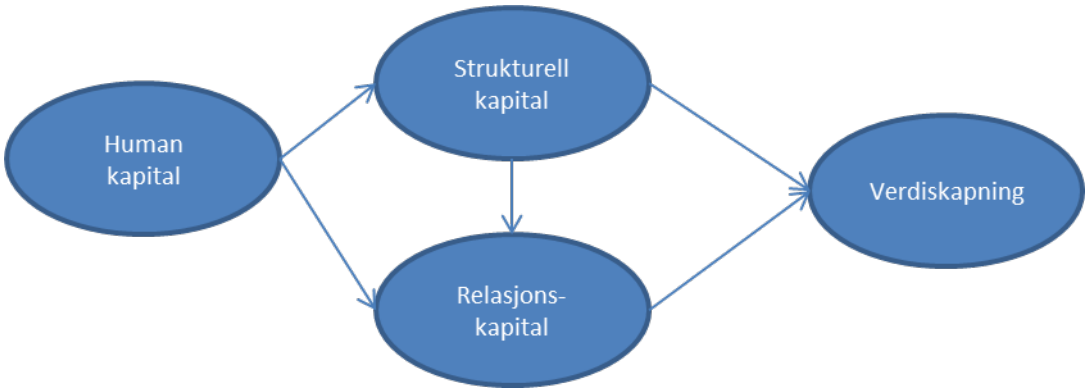
Intellektuell kapital kan klassifiseres som human kapital, strukturell kapital og relasjonskapital (Cabrita & Vaz 2006).

- **Human kapital** er hovedkomponenten i intellektuell kapital. På individuelt nivå består humankapitalen av fire elementer: genetisk arv, utdanning, erfaring og holdninger til livet og til jobben. Humankapitalen er kilden til innovasjon og strategisk fornyelse, hvilket er viktig for både teknologisk innovasjon og organisatorisk omstilling.

- **Strukturell kapital** representerer organisasjonens evne til å møte interne og eksterne utfordringer. Det inkluderer infrastruktur, informasjonssystemer, rutiner, prosedyrer og organisasjonskultur. Strukturell kapital er skjelettet, eller limet, som forsyner organisasjonen med verktøy for å bevare, forflytte og produsere kunnskap. I forhold til strategisk kommunikasjon er den strukturelle kapitalen viktig også for å skape en felles situasjonsforståelse hos alle involverte og å oppnå rask reaksjonsevne.

- **Relasjonskapital** er kunnskap innebygget i relasjoner mellom ulike interessenter som påvirker livet til organisasjonen. Slike relasjoner er nødvendige for å fornye ressurser, prosesser og strukturer over tid, og dermed skape verdi.

Cabrita og Vaz (2006) har laget og testet en forklaringsmodell for hvordan intellektuell kapital innvirker på finansforetaks finansielle og ikke finansielle resultater (Cabrita & Vaz 2006). Modellen viser at humankapitalen virker positivt inn på både strukturell kapital og relasjonskapital, samt at strukturell kapital også virker positivt inn på relasjonskapitalen. Til sist påvirker strukturell kapital og relasjonskapital verdiskapningen og bunnlinjen i selskapet. Innenfor strategisk kommunikasjon vil relasjonskapitalen komme til nytte både internt, i forsvarssektoren, og eksternt, spesielt i forhold til et tettere tverrsektorielt samarbeid på området.



Figur 2.1 Sammenheng mellom intellektuell kapital og verdiskapning

Dersom vi antar at disse relasjonene er allmenngyldige, vil det intuitivt være viktig å bevare og videreutvikle humankapitalen i en organisasjon. Bontis og Fitz-enz (2002) har laget en generisk modell som integrerer intellektuell kapital, knowledge management, human resources, organisatoriske leveranser, IKT og regnskap. Gjennom modellen viser forfatterne hvordan organisasjonen kan beskytte seg mot å tape humankapital (gjennom turnover) ved å investere nettopp i humankapitalen, for eksempel gjennom trening (Bontis and Fitz-enz 2002). Deres forskning understreker betydningen av trening og opplæring, samt en viss stabilitet av kompetanse over tid. Som vi skal se senere, er dette nøkkelfaktorer for å oppnå resultater også i med strategisk kommunikasjon.

Knowledge Management inneholder tre primæraktiviteter (Nonaka and Takeuchi 1995). Disse er:

- **Kunnskapstilvekst**; måten ansatte improviserer og skaper innovasjon på
- **Kunnskapsintegrasjon;** hvordan ansatte overfører sin skjulte kunnskap til eksplisitt kunnskap gjennom å kodifisere ideer inn i systemene til organisasjonen
- **Kunnskapsdeling;** sosialiseringsprosessen der ansatte deler sin kunnskap med andre

Vi vil benytte begrepene og rammeverkene for intellektuell kapital og Knowledge Management for å diskutere Forsvarets utfordringer med strategisk kommunikasjon i kapittel 5. Men først ser vi nærmere på hvilke beredskapsutfordringer og muligheter Norge har med bruk av ikke-kinetiske maktmidler i informasjonsmiljøet.

3 Beredskapsutfordringer og -muligheter

3.1 Krigføring i informasjonsmiljøet

Som vi har sett i kapittel 2.2, innbefatter militære informasjonsoperasjoner et bredt spekter av virkemidler, inkludert psykologiske operasjoner, elektronisk krigføring, datanettverksoperasjoner, villedning og fysiske angrep som ødelegger infrastruktur (Nato 2009b). Krigføring på Balkan, i Irak, i Georgia, i Nord-Afrika og i Midtøsten har illustrert at informasjons- og

kommunikasjonsinfrastruktur er klare militære mål i krig og konflikt, og noe av det første en fiende går til angrep på. På Balkan og i Irak angrep koalisjonsstyrkene elektrisitetsforsyning, TV- og kringkastingsinfrastruktur, og begge sider i disse konfliktene benyttet psykologiske operasjoner med den hensikt å påvirke motparten. Dette understreker behovet for evne til å håndtere bortfall og ulike former for korrumpering av kommunikasjonssystemer. De siste årene har vist at internettet i seg selv er blitt et mål – myndighetene i Syria tok ned internettet for å hindre at opprørere organiserte seg. Facebook og Twitter ble brukt aktivt av begge parter som middel i krigføringen i Gaza, og lokalbefolkning og andre vitner bidrar kontinuerlig til rapportering fra slagmarken. På den digitale slagmarken har også andre grupper engasjert seg, eksempelvis nettaktivister og hackergrupper. Anonymous tok for eksempel palestinernes side i den siste Gaza konflikten, og utførte millioner av angrep mot israelske nettsider (Hagen & Strand 2013). Også Norge – og det norske Forsvaret - må være i stand til å bruke slike digitale plattformer på en mer strategisk målrettet måte i framtiden se kapittel 2.5.

I krig og konflikt utgjør enkeltpersoner, eller grupper med intensjon og kapasitet til å skade, ulike former for trusler. Under et foredrag i Oslo Militære Samfund i februar 2013 delte daværende sjef Cyberforsvaret, generalmajor Roar Sundseth, trusselaktørene inn i tre grupper, alt etter hvilken skade de kan gjøre i cyberdomenet[14] (Windvik, Diesen, Broen, & Johnsen 2013):

1. Kriminelle miljøer er den vanligste og mest omfattende trusselen og disse aktørene retter sin trussel bredt mot hele samfunnet
2. Aktivister har et klart målrettet fokus basert på ideologiske motiver, en kjent aktør er hackergruppen Anonymous
3. Nasjonalstater er den største trusselaktøren som kan forplikte store ressurser over lang tid

Når vi studerer krigføring i informasjonsdomenet, er cyberangrep en sentral del av bildet. Et cyberangrep kan gjennomføres koordinert med andre former for maktmidler, i forkant av eller samtidig som et militært angrep, for å gi en stat en fordel ved å lamme infrastruktur, forsinke mobilisering, spre desinformasjon eller ødelegge militære systemer (Forsvarets stabsskole 2012).

Det er imidlertid flere utfordringer ved å operere i cyberdomenet. De militære utfordringene kan oppsummeres som *attribusjonen* (identifisere fienden), og *den sikkerhetspolitiske konteksten* og *legale utfordringer* i forhold til å drive krigføring i dette domenet (Forsvarets stabsskole 2012). Dessuten er det slik at de aller fleste militære styrker ikke ønsker å eksponere at de bruker offensive cyberangrep (Paul 2008). I tillegg vil vi poengtere at det er stor *usikkerhet* knyttet til konsekvenser av slik krigføring. Et eksempel er Stuxnet, som i følge amerikanske myndigheter, lammet det iranske atomprogrammet i 2010. Etter hvert slo imidlertid dataviruset tilbake på vestens egen kraftproduserende industri og deres kontrollsystemer, og skapte bekymring, men også et sterkere søkelys, på sårbarheter i egen infrastruktur.

[14] Generalmajor Roar Sundseth, Cyberoperasjoner – utfordringer i cyber, foredrag på Olso Militære Samfund 18. februar 2013, http://www.oslomilsamfund.no/oms_arkiv/2013/2013-02-18-Sundtseth.html nedlastet 25.03.2013

Som vi skal se i neste underkapittel, er moderne digitaliserte samfunn som Norge spesielt sårbare for påvirkning. Det at vi publiserer store mengder personlig informasjon på nett gjør det enkelt for en angriper å skaffe seg oversikt over grupper, samt enkeltpersoners holdninger, interesser og vaner. Dette gjør oss mer sårbare. Dessuten har vi over tid opparbeidet en stor grad av tillit til digitale tjenester, og med økende digitalisering øker også avhengigheten av disse tjenestene. Mot dette bakteppet blir det stadig viktigere å ha en klar strategi for å imøtegå eventuelle påvirkningskampanjer i konflikt, krise og krig.

3.2 Sivilsamfunnets sårbarhet og behov for militær assistanse

Norge er en liten stat med en åpen økonomi og åpne grenser geografisk plassert i et fredelig hjørne av verden. Det norske samfunnet er transparent og innbyggerne har stor grad av tillit til hverandre og til staten sammenlignet med andre land (Dehley and Newton 2005). Men denne tilliten i befolkningen er også en bestanddel i vår egen sårbarhet for digital påvirkning. Vi bruker kun to sanser, syn og hørsel, når vi «er på nett» og vi kan derfor i en konfliktsituasjon lett bli et mål for fiendtlig påvirkning. Bruk av internettet og digitale tjenester i alle lag av befolkningen kan også gjøre det enklere å mobilisere massene, og skape engasjement eller motsetninger. Det kanskje mest kjente eksemplet på rask mobilisering ved bruk av digitale tjenester er den arabiske våren, som i stor grad ble drevet fram ved hjelp av internettet og sosiale medier.

Det digitale samfunnet har gitt helt nye kommersielle muligheter for målrettet informasjonsinnhenting og analyse og sammenstilling av store datamengder. Ved hjelp av programvare og algoritmer utvikles systemer som kan søke gjennom det store dypet av data som lagres på eller sendes via nettet. Gjennom algoritmer skapes og identifiseres også trender og forbindelser, blant annet gjennom tilgjengelige digitale fotavtrykk som legges igjen av enkeltpersoner etter internettbruk. De tidligere omtalte eksemplene Google Analytics og Twitter Earthquake Dispatch er to eksempler på hvordan data kan høstes og brukes. Målrettet reklame på Facebook er et velkjent eksempel på utnytting av slike digitale fotavtrykk. Snowden-avsløringene av NSA og GCHQ i 2013 rettet søkelys mot hvordan også nasjoners etterretningstjenester kan utnytte Big data.

Det er vel kjent at Norge er utsatt for spionasje og datalekkasjer. Mørketallsundersøkelsene har over mange år dokumentert at norske virksomheter, både private og offentlige, er utsatt for utstrakt spionasje (Helle et al. 2012). Siste undersøkelse viste at de med immaterielle verdier og de som driver med forskning og utvikling er spesielt utsatt. Også fra sikkerhetstjenestenes egne trusselvurderinger vet vi at spionasje og etterretningstrusselen mot Norge aldri har vært større og at sårbarheten er stor (Forsvaret 2012; Nasjonal sikkerhetsmyndighet 2011; Politiets sikkerhetstjeneste 2013).

Internettet og digitalisering gir mange muligheter for datainnhenting og analyse. Samtidig er tradisjonelle grenser mellom folk og folkeslag bygget ned, og kommunikasjon er stort sett mulig så lenge det finnes en internettforbindelse. Mulighetene for rask informasjonsutveksling har gitt bedre vilkår for ytringsfrihet og rask eksponering av urettferdighet og tragedier.

Men digitalisering av menneskers kommunikasjon seg i mellom har også en skyggeside; individets, virksomheters og samfunnets sårbarhet.

Dagens generasjon har allerede en omfattende digital historikk hvor både interesser, synspunkter og sosialt nettverk kan spores. Samtidig er folks bevissthet om eget privatliv og sensitive personopplysninger på nett, oppsiktsvekkende lav. Gjennom medlemskap i Facebook-grupper, ytringer på Twitter eller gjennom blogging, legges informasjon igjen som i sum kan avsløre mer enn mange kan forestille seg. Foreldre publiserer bilder og hendelser om sine barn, uten å ha tenkt gjennom hva barna vil synes senere, eller hvilke konsekvenser dette kan få for dem på sikt.

En utfordring er at det digitale samfunnet mangler gjemmesteder. Det er vanskelig for forfulgte individer, det være seg politisk forfulgte eller mobbeofre, å starte et nytt liv i den digitale verden. Har du gitt tillatelse til at en tjenestetilbyder lagrer informasjon om deg, kan informasjonen i neste omgang ha blitt distribuert til flere sider. Å få slettet all informasjon er vanskelig, og dersom du «går på nett» igjen kan du spores opp. Selv det som i dag kan virke som gode sikkerhetstiltak, eksempelvis biometri, kan på sikt utgjøre en trussel i denne sammenheng. Med tanke på de siste års datalekkasjer fra ulike virksomheter og databaser, vil konsekvensene av at egne biometriske data kommer på avveie kunne være dramatiske. Hovedutfordringen er at samfunnsutviklingen går med hurtig fart i en retning der vi erstatter direkte mellommenneskelig kontakt med indirekte kontakt via digitale tjenester. Når disse digitale systemene aldri vil kunne ha 100 prosent tette autentiseringssystemer, eller det blir innbrudd i databaser med brukernavn og passord, så er muligheten for identitetstyverier, villedning og svindel betraktelig styrket.

Med så mye potensielt tilgjengelig informasjon om personers interesser, helse og historikk, vil dette igjen gi bedre muligheter for fiendtlig påvirkning. Når interesser og kontaktnett kan spores med et tastetrykk, kan en motpart i neste omgang utnytte dette og gå via venner og bekjente for å utøve påvirkning eller drive utpressing. I en digitalisert verden er dette blitt betraktelig enklere fordi informasjonstilfanget og mulighetene for å bli misbrukt er så store.

Og mens myndighetene vil øke den digitale samhandlingen med folket, er det til sammenlikning begrenset oppmerksomhet rettet mot en helhetlig digital beredskap. Gjeldende politikk tilsier at myndighetene har som mål å være på de digitale arenaene der folket er, det være seg Facebook, Twitter eller andre digitale møteplasser. Men hvilken beredskap har myndighetene hvis disse tjenestene bryter sammen eller informasjon levert via disse blir manipulert, og eventuelt stiller norske myndigheter i et dårlig lys? Hvilken helhetlig beredskap har vi for koordinerte angrep gjennom internettet og digitale medier der informasjon blir endret, folket blir villedet og der viktig kommunikasjonsinfrastruktur ødelegges gjennom fysiske tiltak eller elektronisk inntrenging?

Dette er ikke spørsmål som det finnes noe enkelt svar på, av flere årsaker. For det første har vi aldri erfart et såpass omfattende scenario. For det andre har ikke risikoanalysene statlig og kommunal beredskap bygger på tatt innover seg denne typen scenarioer. For det tredje har slike krisescenarioer aldri vært øvd. Men erfaringene vi *har* gjort oss, inkludert konsekvensene av

enkelthendelser som strømbrudd, feilet programvareoppdatering, uautorisert endring av websider, bildemanipulasjon på nett og nettmobbing etc, tilsier at omfattende konsekvenser må påregnes. Nasjonal sivil beredskap er imidlertid så langt tilpasset enkelttrusler og ikke omfattende koordinerte angrep med flere ulike virkemidler som varer over tid.

Å håndtere sammensatte angrep krever tett koordinering mellom det sivile og det militære, men også internasjonalt samarbeid. Det forutsetter blant annet en helhetlig strategi for utvikling av et konsistent kjernebudskap. Nasjonal beredskap bør derfor, i tillegg til å inkludere Cyberforsvaret og sivil reparasjonsberedskap på infrastruktur, også ha helhetlige kommunikasjonsplaner som beskriver hvordan myndighetene kan nå fram til ulike målgrupper, innbefattet egen befolkning. Planene må ta høyde for bruk av ulike kommunikasjonsplattformer, siden deler av infrastrukturen kan være ute av drift eller upålitelig. Naturkatastrofer de siste årene har vist at det ikke skal mer enn en storm til for å slå ut nasjonal kommunikasjonsinfrastruktur, jamfør stormene Dagmar i 2011 og Ivar i 2013. Men det er ikke bare slike hendelser som kan slå ut digitale systemer. I tråd med økende digitalisering og kompleksitet er det også slik at ordinære driftshendelser, eksempelvis programvareoppdatering kan sette større deler av informasjonsinfrastrukturen ut av spill. De største sviktene relaterer seg til mobilkommunikasjon og internettjenester. Bare i 2012 var det rapportert inn 79 slike store hendelser i EU. De viktigste årsakene var feil i maskinvare, programvarefeil, overbelastning av trafikk og strømbrudd (Mattioli and Dekker 2013).

Feil og naturhendelser kan også oppstå i krise og konfliktsituasjoner, i tillegg til at risikoen for angrep mot kommunikasjonsinfrastruktur generelt øker. For myndighetene vil det være viktig å komme raskt på banen med informasjon til ulike målgrupper og bruke de til enhver tid tilgjengelige digitale og/eller manuelle kommunikasjonskanaler, fra Twitter til konvensjonelle flygeblader. Forsvaret og sivile aktører besitter ulike ressurser og sivilt-militært samarbeid på beredskapssiden vil derfor være av vesentlig betydning i framtiden.

4 Strategisk nivå

4.1 Tverrdepartementalt samvirke og samarbeid

Regjeringen har det overordnete ansvaret for strategisk kommunikasjon. I en krise vil imidlertid det departementet som ut fra sektoransvaret er mest berørt av situasjonen normalt ha koordineringsansvaret for krisehåndteringen. Regjeringen har bestemt at Justis- og beredskapsdepartementet (JD) skal være fast lederdepartement, inntil Regjeringen bestemmer noe annet. Avhengig av situasjonens art vil de mest sentrale departementer da være JD, Utenriksdepartementet (UD) eller Forsvarsdepartementet (FD). I tillegg vil Statsministerens kontor (SMK), i henhold til planverket for Sivilt beredskapssystem, ha et særskilt ansvar for informasjonsberedskap. SMK vil alltid kunne ta særskilte initiativer for å koordinere eller legge føringer.

I internasjonale konflikter og i prosessen med å sette sammen et situasjonsbilde, vil ambassadenes medieovervåkning kunne gi verdifulle innspill til situasjonsforståelsen, og dermed også til den

strategiske kommunikasjonsplattformen. I dette vil også Nato-kanalene, herunder Norges delegasjon til Nato (Nordel) og Norges militærmisjon i Brussel (MMB), være viktige bidragsytere. De nasjonale delegasjonene har også potensielt en sentral rolle å spille i "oversettelsen" av Natos overordnete narrativer slik at de resonnerer best mulig i norske målgrupper.

FFIs forskning har avdekket at effektiv strategisk kommunikasjon i en operasjon forutsetter et klart budskap som har sin opprinnelse i politiske mål (Søgaard og Hagen 2013). Dette kjernebudskapet må være konsistent over tid, og er avhengig av en rød tråd fra politisk nivå og helt ned til Forsvarets utøvende ledd for mest mulig optimal effekt. Dersom opinionen oppfatter at militære handlinger ikke samsvarer med de uttrykte politiske mål, risikerer troverdigheten – og støtten – til operasjonen å bli kraftig svekket og, i verste fall, true utfallet. Spesielt siden situasjonen angår langt flere, inkludert sivile instanser, kan ikke Forsvaret lage en ensidig plan. Derfor må ansvaret for budskapsplattform og rød tråd forankres både horisontalt (UD, JD, Helse- og omsorgsdepartementet (HOD) med flere) - og, ikke minst, vertikalt oppover, til SMK og nedover gjennom hele Forsvarets organisasjon. UD vil være spesielt viktig fordi det er deres oppgave å vinne gehør for norske synspunkter internasjonalt. Et slikt tett og løpende tverrsektorielt samarbeid er helt avgjørende for å sikre konsistente budskap, og at aktørene framstår som samstemte. I dette vil *formelle koordineringsprosedyrer* forankret hos beslutningstakerne være av betydning for at dette konsistente budskapet skal kunne formidles så tidlig som mulig, helst allerede i eskaleringsfasen av en konflikt (Søgård and Hagen 2013). Men slike prosedyrer vil også være av vesentlig betydning for en vellykket krisehåndtering av et eventuelt narrativsbrudd i etterkant.

Alt dette forutsetter at det i framtiden vil være enda viktigere med øving på krisehåndtering i forhold til digitale trusler og strategisk kommunikasjon. Gjennom øving og trening kan problemer avdekkes, for eksempel mangel på kompetanse og systemer, og nye løsninger kan bli utviklet. Som beskrevet i kapittel 2.6, vil dette også bidra til at humankapitalen vokser, noe som i sin tur vil gi bedre strukturell kapital og relasjonskapital innenfor området krisehåndtering og nasjonal beredskap, jfr (Cabrita & Vaz 2006).

4.2 Utfordringer for Forsvaret på strategisk nivå

Hvordan håndtere utfordringer knyttet til strategisk kommunikasjon vil være en viktig problemstilling for Forsvaret ved en sikkerhetspolitisk krise eller krig på norsk territorium. Et moment er at stratkom lett blir oppfattet som propaganda, selv om det i følge (Tatham 2008) er grunnleggende ulikheter mellom de to. En annen utfordring er hvordan planlegge og måle effektiv strategisk kommunikasjon innenfor en global verdens uoversiktlige rammebetingelser (Hylland-Eriksen 2007). Som vi poengterte i kapittel 2.4, illustrerer Hylland-Eriksens globaliseringsdimensjoner den nye tids krav til hurtighet, reaksjonsevne, persepsjon og situasjonsforståelse, og ikke minst, kompleksiteten i å nå ulike målgrupper, og å påvirke andre grupper utilsiktet.

I Norge skisserer Direktiv for kommunikasjonsvirksomhet i Forsvarssektoren (17. april 2013) ansvars- og myndighetsområder, målgrupper, definisjoner, særskilte roller og funksjoner, og gjelder for hele krisespektret. Det pågår også et arbeid med å utvikle beredskapsplaner på området. Men dette planverket stiller også stadig strengere krav til fagansvarlige innenfor strategisk kommunikasjon om hva dette krever av Forsvaret som organisasjon generelt, og Forsvarets kommunikasjonsvirksomhet spesielt. I dette vil analyseverktøy være et vesentlig hjelpemiddel for maksimal effekt av de tiltak som iverksettes.

Som påpekt i kapittel 2 kan intellektuell kapital klassifiseres som henholdsvis human kapital, strukturell kapital og relasjonskapital. Intellektuell kapital har stor betydning for verdiskapning og leveranser til organisasjonen. Kan utfordringer knyttet til strategisk kommunikasjon i Forsvaret forstås bedre i lys av dette begrepsapparatet?

Humankapital: Som påpekt tidligere handler strategisk kommunikasjon mer om langsiktig *strategi* enn *kommunikasjon* eller *kanaler*. Effektiv strategisk kommunikasjon forutsetter derfor relevant kompetanse, som oppnås gjennom daglig arbeid, kursing, formell utdannelse, øvelser og rekruttering. Øvelser er viktige fordi kommunikasjonspersonell i Forsvaret i det daglige ofte tvinges til å prioritere det løpende nyhetsbildet (Søgaard og Hagen, 2013). Øvelser vil derfor være en viktig arena for at den strategiske dimensjonen også blir ivaretatt og utviklet. I sin enkleste form kan miniseminarer eller skrivebordsøvelser brukes til å diskutere mål, målgrupper og kommunikasjonsstrategier i ulike scenarioer. Gjennom øvelser kan kunnskap bli utviklet og medarbeidere kan improvisere og være kreative på ufarlige arenaer. Øvelser gir også muligheter for kunnskapsdeling gjennom sosialisering og nettverksbygging. Et annet kompetansebyggende tiltak er kurs i regi av Nato eller Nato-partnere, og bevisst rekruttering av nye medarbeidere med erfaring fra for eksempel utenlandsoperasjoner. Å tilby opplæring og trening reduserer videre faren for tap av kompetanse ved at folk slutter (Bontis & Fitz-enz 2002). FFI har gjennom prosjektet ”Militære informasjonsoperasjoner” avdekket at det er et sterkt ønske blant Forsvarets egne om mer kursing og trening på området (Søgaard & Hagen 2013).

Strukturkapital: I utgangspunktet har Forsvarets prosedyrer og plandokumenter, beredskapsplanverk og rammeavtaler potensial for å gi sentrale strukturelle forutsetninger for strategisk kommunikasjon. Planprosessene foregår løpende i forkant av de årlige militære øvelsene. FFI har imidlertid avdekket at strategisk kommunikasjon og informasjonsoperasjoner kun har hatt en begrenset plass i disse planleggingssyklusene så langt. For å lykkes bør stratkom integreres i stridshjulet fra første stund. Det forutsetter en sterkere kopling mellom politikkutforming, kommunikasjonsvirksomheten og militære planleggere. I følge Bøe-Hansen bør stratkom-prosessen forankres gjennom planverk, løpende prosesser og institusjoner, noe som ikke er tilfelle i Norge i dag. En mulig modell til inspirasjon er Storbritannias National Security Council, hvor rammene for strategisk kommunikasjon i krisehåndtering diskuteres i ukentlige møter under ledelse av statsministeren (MoD 2012). En formalisering av et tverrsektorielt stratkom-samarbeid vil også kunne styrke de formelle samarbeidsrelasjonene i Norge (Bøe-Hansen 2013).

Kommunikasjonsvirksomheten i Forsvaret er kommet et godt stykke på vei i oppdatering av eget planverk, inkludert retningslinjer, samt direktiv og beredskapsplan for kommunikasjonsvirksomheten. Men for at beskrivelser av roller, ansvar og myndighet, horisontalt og vertikalt, skal ha en reell effekt, må planene øves i fredstid. Det er også viktig å få på plass rammeavtaler med relevante samarbeidspartnere. Dagens globaliserte verden krever en betydelig større grad av planlegging og samordning enn det som var nødvendig under den kalde krigen (Hylland-Eriksen 2007). Den gang hadde vi et mindre sammensatt trusselbilde, vi hadde et invasjonsforsvar og hovedsakelig én fiende. I dag kan fienden like gjerne være midt i blant oss som hos en utenlandsk aktør. Terrorgrupper er bare et eksempel på det. Det er vanskelig å beskytte seg mot terror og opprør, og en større og mer mangfoldig verktøykasse for ikke-kinetisk maktbruk er derfor påkrevet.

I tillegg til et relevant og oppdatert beredskapsplanverk, er det behov for analyseverktøy som kan hjelpe fagfolk til å gjøre strategiske vurderinger av kommunikasjonseffekten. Den digitale utviklingen har åpnet opp et bredt spenn av muligheter, men det innebærer også at kravet til hurtig respons stadig blir viktigere. Strategisk satsing på mer proaktiv bruk av sosiale medier i direkte kommunikasjon med befolkningen er et resultat av dette. For eksempel tok Forsvarets kommunikasjonsvirksomheten i bruk Twitter for å imøtegå kritisk omtale av Regjeringens kampflyprosjekt i en NRK-dokumentar i april 2013[15]. Men det kan også være nyttig å trekke på erfaringer fra digitalt nødhjelpsarbeid, der crowdsourcing, BigData-analyse, crisismapping og digital datainnhenting, er blant ingrediensene. Dette representerer viktige skritt videre i utnytting av sosiale medier. Denne teknologien kan brukes til å gi myndigheter og befolkning et bedre situasjonsbilde og en bedre overvåking av utviklingen politisk, militært, økonomisk, sosialt, informasjonsmessig og infrastrukturelt. På dette området er det utvilsomt et enda større potensialet for nytenkning i forhold til strategisk kommunikasjon- og for nasjonal digital beredskap.

Relasjonskapital: Strategisk kommunikasjon kan ikke planlegges og utøves av Forsvaret alene, heller ikke i de tilfeller hvor Forsvarsdepartementet er lederdepartement. Som gjort rede for under kapittel 2.3, kan nasjoner ta i bruk ulike maktmidler i krisesituasjoner, eksempelvis innenfor diplomati, informasjon, militære og økonomiske (DIME). For å oppnå mest mulig effekt av den strategiske kommunikasjonen, må et felles overordnet budskap og et støttende narrativ være på plass og formidles innen alle disse fire områdene. En slik helhetlig tilnærming forutsetter imidlertid en kommunikasjonsstrategi som inkluderer hele Forsvaret, andre departementer og eventuelle koalisjonspartnere (Försvarsmakten 2008). Uten en slik strategi er faren for kommunikasjon med flere tunger overhengende. Det kan igjen resultere i at det overordnete kjernebudskapet eller narrativet brytes. I følge Bøe-Hansen er dette det verste som kan skje innen strategisk kommunikasjon (Bøe-Hansen 2013). Og som nevnt tidligere, vil en helhetlig kommunikasjonsstrategi også være en forutsetning for en vellykket håndtering i etterkant av et eventuelt narrativsbrudd.

[15] Erik Tornes: ”Journalistikk under angrep”, kommentarartikkel i Aftenposten 20. april 2013.

Strategisk kommunikasjon kan heller ikke sees isolert fra resten av virksomheten, men må være en integrert del av alt Forsvaret foretar seg, også i fredstid. Det forutsetter tett samordning mellom taktisk, operasjonelt og strategisk nivå i Forsvaret, men også koordinering eksternt med andre departementer og sektorer. Og for at kommunikasjonsrådgivere skal kunne gi solide strategiske råd i operasjonsplanlegging, må disse integreres fra første stund i alle planprosesser. Strategisk kommunikasjon bør med andre ord ha en like naturlig plass i stridshjulet som klassiske kinetiske maktmidler, og ikke kun dekkes i et appendiks "litt på siden" av helheten – slik det har vært en tendens til så langt.

4.3 Strategisk kommunikasjon i strid

I krise eller krig vil det være avgjørende for utfallet at alle virkemidlene som tas i bruk kommuniserer et budskap som er konsistent med det overordnete narrativet. I dette vil en overordnet kommunikasjonsstrategi som omfatter samtlige myndighetsinstanser nasjonalt, i tillegg til eventuelle koalisjonspartnere og andre samarbeidsorganer, være av vesentlig betydning (Försvarsmakten 2008). Dersom en slik helhetlig strategi ikke er på plass, er risikoen for å kommunisere med «flere tunger» tilstede, noe som kan gi meget uheldige utfall (Fenton 2012).

Som tidligere påpekt, vil Natos policy innen strategisk kommunikasjon gjelde i alle Nato-operasjoner, inklusive operasjoner på norsk territorium. I følge Grandhagen er stratkom i Nato en prosess og en koordinerende funksjon som dels er en sentral del av den politiske og militære planprosessen, og dels er analyserende og korrigerende når det gjelder pågående militære operasjoner. Videre sier Grandhagen at den militære operative planleggingens mål er å identifisere motstanderens tyngdepunkt, og når dette er gjort, benytte tilgjengelige virkemidler for å ramme dette tyngdepunktet slik at motstanderen ikke er i stand til selv å utføre egne operasjoner. I opprørsbekjempelse er motstanderens tyngdepunkt knyttet til vilje, ideologi og motivasjon. Siden strategisk kommunikasjon påvirker menneskene kognitivt, vil strategisk kommunikasjon derfor kunne være en sentral faktor for påvirke sluttresultatet og å avmilitarisere operasjonsmålene (Grandhagen 2011).

Som påpekt av Paul, Clarke og Grill kan strategisk kommunikasjon i opprørsbekjempelse bidra til suksess (Paul, Clarke, & Grill 2010). Grandhagen slår fast betydningen av at den militære og politiske oppdragsprosessen er omfattet av samme grunnleggende kommunikasjonsmål og plan slik at det ikke utvikler seg motstridende budskap og handlinger på lavere nivå. Optimalt skal mål og retningslinjer som legges på strategisk nivå, ende opp i konkrete planer, ordrer og handling helt ut i organisasjonens utøvende ledd (Grandhagen 2011).

I Norge er FD ansvarlig for det overordnete militære narrativet og de militære responsopsjonene (MRO). Deretter skal disse responsopsjonene vurderes på militærstrategisk nivå i Forsvaret, før det blir utstedet en varslingsordre nedover til operasjonelt nivå. Det er dermed lagt til rette for strategisk kommunikasjon kan integreres i den militære operasjonsplanleggingen.

På taktisk nivå vil målgruppeanalyser være sentralt for å "treffe" riktig. Men det kan være utfordrende å isolere målgrupper i en digitalisert verden (Sandrup 2013).

Hvordan forstå forskjellen på den strategisk viktige meldingen, og den taktisk ubetydelige meldingen, samt hvilken innvirkning disse kan ha på en situasjon (Nissen 2011)? Også i disse prosessene vil digitale analyseverktøy kunne være nyttige for å oppdatere situasjonsbildet og løpende effektvurderinger.

5 Konklusjon og videre arbeid

Rapporten har dekket tre temaer:

Strategisk kommunikasjon som ressurs for krisehåndtering i informasjonsmiljøet.
I gjennomføringen av langtidsplanen Prop. 73 S (2011–2012) ”Et forsvar for vår tid” fastslår norske myndigheter at de særlig vil ”styrke Forsvarets evne til å utgjøre en krigsforebyggende terskel gjennom å videreutvikle Forsvarets samlede kapabiliteter og betrakte militære evner i et helhetlig perspektiv, både nasjonalt og i en alliert kontekst” (Forsvarsdepartementet 2012a). Vi mener strategisk kommunikasjon vil kunne understøtte denne oppgaven i fredstid på samme måte som strategisk kommunikasjon har understøttet militær opprørsbekjempelse (Paul, Clarke, & Grill 2010). Det forutsetter imidlertid en helhetlig tilnærming, inkludert større bevissthet rundt mulighetsrom og utfordringer for strategisk kommunikasjon i en global og digitalisert verden. I krigsforebygging, som i opprørsbekjempelse, ligger mye av tyngdepunktet i en militær operasjon i det kognitive domenet, det vil si i menneskers holdninger og meninger. Når målgrupper og mål er identifisert, vil neste trinn kunne være å utvikle en strategi og tilhørende virkemidler (DIME), som eksempelvis kan brukes til å påvirke målgrupper langs ulike dimensjoner (PMESII). I dette vil det være avgjørende å gjøre grundige konsekvensanalyser. Digitale analyseverktøy og høsting av data på nett gir helt nye muligheter for målinger og konsekvensanalyser, og har potensial til å gi merverdi også innen stratkom.

Strategisk kommunikasjon som merverdi for Forsvaret i fredsdrift og i militære operasjoner.
Nato har lenge benyttet strategisk kommunikasjon i sine operasjoner, og som Nato-medlem er Natos policy på området gjeldende også for Norge. Strategisk kommunikasjon har også vist seg å være en bidragsyter til suksess i forbindelse med blant annet internasjonal opprørsbekjempelse (Paul, Clarke, & Grill 2010). Likevel har FFIs forskning avdekket at stratkom ikke er en integrert del av Forsvarets planprosesser når det virkelig gjelder. Dette vil imidlertid være viktig for at Norge også i framtiden skal kunne støtte opp under Natos satsing på området. Natos uttalte mål er å sette informasjonsstrategier i sentrum på alle nivå av policy, planlegging og implementering, for på den måten å bidra til praktiske og effektive strategier som bidrar til suksess (Bøe-Hansen 2013). Dette forutsetter ikke nødvendigvis flere ressurser, men videreutvikling av metoder og prosesser som allerede eksisterer. I tillegg kreves nytenking rundt hva påvirkning innebærer i et mangfoldig og uoversiktlig informasjonssamfunn. Dette er kanskje spesielt viktig for Norge som en småstat med mektige naboer som har økende interesser i Nordområdene. I en gitt situasjon ”vil Norges reelle maktmidler i framtiden være internasjonal rett, politisk og diplomatisk kreativitet og kløkt, og regional og internasjonal legitimitet, snarere enn tradisjonell og militær militærmakt” (Dyndahl and Simonsen 2013). Også i et slikt perspektiv vil strategisk kommunikasjon med bruk av relevante virkemidler kunne være en viktig brikke for å nå sikkerhetspolitiske mål.

Utfordringer og muligheter relatert til strategisk kommunikasjon.
Forsvaret står overfor en rekke utfordringer knyttet til strategisk kommunikasjon og digital påvirkning. Den første er diskursen rundt påvirkning i Nato, som i Norge ofte assosieres med politisk sensitive begreper som propaganda. Strategisk kommunikasjon beskriver hvordan handling skal bygge opp under narrativer, i motsetning til propaganda, som kun dreier seg om ord. Den andre utfordringen er at hvordan vi måler effekten av strategisk kommunikasjon i en global verden, hvor målgrupper endrer seg og flytter på seg, og hvor budskapet når ut i verden i løpet av sekunder. Disse rammebetingelsene krever god situasjonsforståelse og stiller strenge krav til metodebruk og konsekvensanalyser. Andre utfordringer er relatert til Forsvarets intellektuelle kapital på området og til Forsvarets utøvelse av Knowledge Management. FFIs forskning har avdekket at strategisk kommunikasjon i Forsvaret så langt har vært svært avhengig av enkeltpersoners innsats (Søgaard & Hagen 2013). For å sikre kontinuitet bør Forsvaret styrke humankapitalen gjennom trening, utdanning og bevisst rekruttering. Mer trening og øvelser kan videre bidra til å redusere eventuell turnover og til å gi mulighet å videreutvikle kvaliteten på den strategiske kommunikasjonen.

Innenfor dimensjonene strukturell kapital og relasjonskapital har vi avdekket utvalgte forbedringsområder. Strategisk kommunikasjon forutsetter samarbeid på tvers av myndighetsområder. I dag blir slike hensyn i noen grad ivaretatt av Kriserådet, men en tilnærming som tilsvarer det britiske nasjonale kriserådet ville i enda større grad ha sikret den tverrsektorielle samordningen som er helt avgjørende for å lykkes. En tydeligere formalisering av samarbeid på tvers av myndighetsinstanser vil derfor være sentralt dersom målet er effektiv strategisk kommunikasjon.

Norge er et lite land med små fagmiljøer. Det burde derfor være en overkommelig oppgave å bygge relasjonskompetanse innenfor strategisk kommunikasjon. Det pågår arbeid med beredskapsplaner, som må øves før de blir effektive og brukbare. Øving er også viktig for å få til overføring av kompetanse og kunnskap mellom ulike profesjoner og avdelinger, og for å bygge relasjoner. Utdanning, kursing og trening av personell, eksempelvis i Nato-regi vil også bidra til å øke den intellektuelle kapitalen på fagområdet.

Videre forskning:
Det er behov for videre forskning på bruk av ikke-kinetiske maktmidler innen krisehåndtering, inkludert militære informasjonsoperasjoner og strategisk kommunikasjon som ledd i forsvarskampen. I FFIs arbeid for operasjonelt nivå har det blitt identifisert behov for klarere føringer fra strategisk nivå til operativt nivå i Forsvaret. Det er også identifisert behov for å skaffe oversikt over prosesser, dokumenter og metoder som beskriver og referer til strategisk kommunikasjon og informasjonsoperasjoner. Videre er det avdekket behov for å utforske ulike modeller for organisering (roller, ansvar og myndighet) og ledelse av strategisk kommunikasjon, spesielt i tilknytning til tverr-sektorielt samarbeid. Sist, men ikke minst, er det avdekket et sterkt behov for analyseverktøy og metoder som kan bidra til et bedre situasjonsbilde og bedre forutsetninger for å gjøre strategiske effektvurdering av ikke-kinetiske maktmidler. Her åpner økt digitalisering, bruk av sosiale medier og analyser av Big data opp et helt nytt mulighetsrom.

Litteratur

Bagdikian, B. H. War, Media, and Propaganda. A Global Perspective, Foreword, Maryland, United States of America: Rowman & Littlefield Publishers, Inc., p. xi-xiii.

Bøe-Hansen, O. 2013, "Strategisk kommunikasjon i en norsk kontekst," *In Militærstrategi på norsk*, H. Edstrøm & P. Ydstebø, eds., Oslo: Abstrakt forlag, pp. 349-350.

Bontis, N. & Fitz-enz, J. 2002. Intellectual capital ROI: a causal map of human capital antecedents and consequents. *Journal of intellectual Capital*, 3, (3) 223-247

Cabrita, M.d.R. & Vaz, J.L. 2006. Intellectual Capital and value Creation: evidence from the Portuguese Banking Industry. *the Electronic Journal of Knowledge Management*, 4, (1) 11-20

Dehley, J. & Newton, K. 2005. Predicting Cross-National Levels of Social Trust: Global Patterns of Nordic Exceptionalism? *European Sociological Review*, 21, (4) 311-327

Dyndahl, G. L. & Simonsen, S. Krisehåndtering i fiskerivernsonen - mellom jus og interessepolitikk. Norsk Militært Tidsskrift [1]. 2013.

Fenton, T. 2012, "Thoughts on Journalism and the Military," G. J. David Jr. & T. R. McKeldin, eds., Dulles, Virginia: Potomac Books Inc, pp. 87-92.

Forsvaret 2012, *FOKUS 2012. Etterretningstjenestens vurdering.*

Forsvarets stabsskole 2012. *Innblikk i fellesoperasjoner - synergi gjennom felles innsats* Forsvaret.

Forsvarsdepartementet. Et forsvar for vår tid. Prop. 73 S (2011-2012). 2012a.

Forsvarsdepartementet. Et forsvar til vern om Norges sikkerhet, interesser og verdier. St.prp. nr. 48 (2007-2008). 2012b.

Försvarsmakten 2008, *Försvarsmaktens Handbok Informationsoperationer*, Försvarsmakten Högkvarteret, Stockholm, 2008-01-24 utgåva MF7739-352014.

Grandhagen, K. H. 2011, *Fra målløst prat til strategisk kommunikasjon. Utviklingen av Natos strategiske kommunikasjonskonsept og Norges evne til å ta del i konseptet. Masteroppgave*, Forsvarets høgskole.

Hagen, J. M. & Strand, O. M. 2013, *Det digitale samfunnet: Vår egen sårbarhet for militære informasjonsoperasjoner FFI-Rapport 2013/00883 BEGRENSET*, Forsvarets forskningsinstitutt, FFI-Rapport 2013/00883.

Haugen, K. 2011, *Strategisk kommunikasjon. En analyse av ekstern kommunikasjon i Nato. Masteroppgave*, Forsvarets høgskole.

Helle, A.-J., Birkeland, C., Ofigsbø, E., Hagen, J., Mathiesen, J., Folkedal, H., Orderløkken, T. L., Østmo, V., Thingbø, T., & Beitland, K. 2012, *Mørketallsundersøkelsen 2012. Informasjonssikkerhet og datakriminalitet.*, Næringslivets sikkerhetsråd, Oslo.

Hubbard, Z. P. 2007, "Information Operations in the Global War on Terror: Lessons Learned From Operations in Afghanistan and Iraq," *In Information Warfare. Separating hype from reality*, L. Armistead, ed., Dulles, Virginia: Potomac Books Inc, pp. 45-72.

Hylland Eriksen, T. 2007. *Globalization - the Key Concept* Oxford, New York, Berg.

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H., & Thurston, C. Q. 2009, *Foundations of Effective Influence Operations. A framework for Enhancing Army Capabilities.*, RAND Corporation, Santa Monica.

Livingston, S. 1997, *Clarifying the CNN Effect: An Examination of Media Effects According to Type of Military Intervention, Research Paper R-18*, The Joan Shorenstein Center, Harward University, Cambridge.

Manheim, J.B. 2012. *Strategy in Information and Influence Campaign. How policy advocates, social movements, insurgent groups, corporate governments and others get what they want* New York and London, Routledge, Taylor & Francis Group.

Mattioli, R. & Dekker, M. 2013, *National roaming for mitigating mobile network outages*, European Union for Network anhd Information Security (ENISA), Heraklion, Hellas.

Mc Fate, M. The Military Utility of Understanding Adversary Culture. Joint Force Quarterly [38], 42-48. 2005. Washington DC, National Defence University Press.

MoD 2012, *Joint Doctrine Note 1/12 Strategic Communication The Defence Contribution*, Ministry of Defence, Shrivenham, UK.

Munoz, A. 2013, *U.S. Military Information Operations in Afghanistan. Effectiveness of Psycological operations 2001-2010*, RAND, Santa Monica, CA.

Nasjonal sikkerhetsmyndighet 2011, *Rapport om sikkerhetstilstanden*, Nasjonal sikkerhetsmyndighet.

Nato. ACO Strategic Communication, ACO Directive (AD) 95-2. ACO Directive (AD) 95-2. 2009a.

Nato 2009b, *Allied Joint Doctrine for Information Operations, AJP 3.10*, Nato.

Nato. Military Concept for NATO Strategic Communication, Nato Unclassified. 2010. Brussels, Nato.

Nato. Nato Military Policy on Information Operations. Military Decision on MC 0422/4, 20. July 2012, Nato Unrestricted. 2012.

Nissen, T. E. 2011, *Tactical Information Operations in Contemporary COIN Campaigns*, Forsvarsakademiet, Copenhagen.

Nonaka, I. & Takeuchi, H. 1995. *The Knowledge-Creating Company* New York, Oxford university Press.

Paul, C. 2008, *Information Operations. Doctrine and Practice. A Reference Handbook.*, Praeger Security International, Westport, USA.

Paul, C., Clarke, C. P., & Grill, B. 2010, *Victory Has a Thousand Fathers. Sources of Success in Counterinsurgency*, National Defense Research Institute (RAND), Santa Monica, CA.

Politiets sikkerhetstjeneste 2013, *Trusselvurdering 2012*, Politiets sikkerhetstjeneste, Oslo.

Richter, W. E. The future of information operations. Military Review [January-February], 103-113. 2009.

Sandrup, T. 2013, *(U) PSYOPS som virkemiddel - refleksjoner rundt norske erfaringer fra Afghanistan, FFI-Rapport 2013/01502, BEGRENSET*, Forsvarets forskningsinstitutt.

Siegel, P.C. 1998. *Target Bosnia: Integrating Information Activities in Peace Operations. NATO-Led Operations In Bosnia-Herzegovina. December 1995-1997* Washington, Institute for National Strategic Studies: NDU Press.

Søgård, H. A. & Hagen, J. M. 2013, *Strategisk kommunikasjon i praksis - utfordringer for Forsvarets sentrale kommunikasjonsvirksomhet, FFI-Rapport 2013/01253, BEGRENSET*, Forsvarets forskningstitutt.

Tatham, S. A. Strategic Communication: A primer. 2008. Swindon, Defence Academy of United Kingdom, Advanced Research and Assessment Group.

Time, A. S. 2012, *Tilbakemeldinger fra media på politiets informasjonsarbeid og mediehåndtering ifm 22. juli 2011. For Politidirektoratet.*, Geelmuyden Kiese, Oslo.

Ward, B. M. 2003, *Strategic influence operations - the information connection (Unclassified)*, U.S Army War College, Pennsylvania.

Windvik, R., Diesen, S., Broen, T., & Johnsen, S. T. 2013, *Cyberdomenet - cyberoperasjoner og cybermakt, FFI-rapport 2013/01125 BEGRENSET*, Forsvarets forskningsinstitutt.

Forkortelser

Forkortelse	Forklaring
CIA	Central Intelligence Agency
CNA	Computer Network Attacks
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COP-D	Comprehensive Planning Directive
DIME	Diplomacy, Information, Military, Economy
EK	Elektronisk krigføring
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
HOD	Helse- og omsorgsdepartementet
IA	Information Activities
IDF	Israel Defence Forces
INFOSEC	Information Security
IO	Informasjonsoperasjoner
JD	Justisdepartementet
MoD	Ministry of Defence
MRO	Militære Responsopsjoner
NAC	North Atlantic Council
Nato	North Atlantic Treaty Organization
NSA	National Security Agency
OPSEC	Operation Security
PA	Public Affairs
PMESII	Political Military Economic Social Information Infrastructure
PSYOPS	Psykologiske operasjoner
SMK	Statsministerens kontor
UD	Utenriksdepartementet
UK	United Kingdom