Air Power in Future Joint Operations – A Multi-Domain Battle?

Luftkrigsskolens skriftserie Vol. 35

Andre utgivelser i skriftserien:

Vol. 1 Luftforsvaret— et flerbruksverktøy for den kalde krigen? (1999)
Øistein Espenes & Nils Naastad

Vol. 2 Aspekter ved konflikt og konflikthåndtering i Kosovo (2000)
Gunnar Fermann

Vol. 3 Nytt NATO — nytt Luftforsvar?: GILs luftmaktseminar 2000 (2000)
Lars Fredrik Moe Øksendal (red.)

Vol. 4 Luftkampen sett og vurdert fra Beograd (2000)
Ljubisa Rajik

Vol. 5 Luftforsvaret i fremtiden: nisjeverktøy for NATO eller multiverktøy for Norge? (2001)
John Andreas Olsen

Vol. 6 Litteratur om norsk luftfart for 2. verdenskrig: en oversikt og bibliografi (2001)
Ole Jørgen Maaø

Vol. 7 A critique of the Norwegian air power doctrine (2002)
Albert Jensen & Terje Korsnes

Vol. 8 Luftmakt, Luftforsvarets og assymetriens utfordringer. GILs luftmaktseminar 2002 (2002)
Karl Erik Haug (red.)

Vol. 9 Krigen mot Irak: noen perspektiver på bruken av luftmakt (2003)
Morten Karlsen, Ole Jørgen Maaø & Nils Naastad

Vol. 10 Luftmakt 2020: fremtidige konflikter. GILs luftmaktseminar 2003 (2003)
Karl Selanger (red.)

Vol. 11 Luftforsvaret og moderne transformasjon: dagens valg, morgendagens tvangstrøye? (2003)
Ole Jørgen Maaø (red.)

Vol. 12 Luftforsvaret i krig: ledererfaringer og menneskelige betraktninger.
GILs lederskapsseminar 2003 (2003) Bjørn Magne Smedsrud (red.)

Vol. 13 Strategisk overraskelse sett i lys av Weserübung, Pearl Harbor og Oktoberkrigen (2005)
Steinar Larsen

Vol. 14 Luftforsvaret i Kongo 1960—1964 (2005) Ståle Schirmer-Michalsen (red.)

Vol. 15 Luftforsvarets helikopterengasjement i internasjonale operasjoner:
et historisk tilbakeblikk (2005) Ståle Schirmer-Michalsen

Vol. 16 Nytt kampfly— Hvilket og til hva? GILs luftmaktseminar 2007 (2007)
Torgeir E. Sæveraas (red.)

Vol. 17 Trenchard & Slessor: On the Supremacy of Air Power over Sea Power (2007)
Gjert Lage Dyndal

Vol. 18 På vei mot en militær bachelor. En antologi av kadetter ved Luftkrigsskolen (2008)

Vol. 19 Norsk luftmakt — tilbake til fremtiden? GILs luftmaktseminar 2008 (2008)
Torgeir E. Sæveraas & Albert Jensen (red.)

Vol. 20 Vilhelm Mohr. On World War II (2009) Dag Henriksen

Vol. 21 Luftmakt og teknologi- realisme eller overmot? Hvilken effekt har moderne teknologi i krig? GILs LUFTMAKTSEMINAR 2009 (2009).
Per Marius Frost-Nielsen & Torgeir E. Sæveraas (red.)

Vol. 22 The 1970— 1974 Combat Aircraft Analysis. Priority to Defensive Counter Air and Anti-Shipping
Operations. How optimizing defence resources altered the use of RNoAF fighters (2010). Hans Ole Sandnes

Vol. 23 8 år i Afghanistan, Quo Vadis? Et seminar om militær maktanvendelse.
GILs LUFTMAKTSEMINAR 2010 (2011).
Torgeir E. Sæveraas (red.)

Vol. 24 Norske luftmaktstenkere 1926—1940. En presentasjon av fem sentrale skribenter og deres arbeid
Frode Lindgjerdet

Vol. 25 Etter Afghanistan — Ny strategisk virkelighet? GILs LUFTMAKTSEMINAR 2011(2012), Torgeir E. Sæveraas (red.)

Vol. 26 Luftmakstenkningens «enfant terrible». Festskrift til Nils E. Naastad på 60-årsdagen.
Øistein Espenes & Ole Jørgen Maaø (red.)

Vol. 27 Norsk luftmakt over Libya — suksess uten innflytelse? GILs Luftmaktseminar 2012 (2012).
Torgeir E. Sæveraas & Vidar Løw Owesen (red.).

Vol. 28 Norske kampfly i operation enduring freedom, Afghanistan 2002-2003. Politisk kontroll og engasjementsregler (2013).
Per Marius Frost-Nilsen

Vol. 29 UAV - bare av teknologi eller en ny strategisk virkelighet?
GILs LUFTMAKTSEMINAR 2013. Torgeir E. Sæveraas & Marianne Eidem (red.)

Vol. 30 Ledelse av norsk luftmakt: En alliert eller norsk oppgave? GILs LUFTMAKTSEMINAR 2014.
Torgeir E. Sæveraas & Dag Inge Korstad (red.).

Vol. 31 Endringskapasitet og lederskap. Luftkrigsskolens lederskapsseminar 2013
Ingunn Dahler Hybertsen & Trygve Jakobsen Steiro (Red.)

Vol. 32 A New Russia? Consequences for Norway and the Royal Norwegian Air Force?
Torgeir E. Sæveraas (red.)

Vol. 33 NATO: Challenges and Solutions – GILs luftmaktseminar 2016
Torgeir E. Sæveraas (red.)

Vol. 34 Evolution to a 5th Generation Air Force – Norway's Shield and Sword?
Ann Karin Larssen (red.)

Air Power in Future Joint Operations – A Multi-Domain Battle?

Sjef Luftforsvarets luftmaktseminar 2018

Ann Karin Larssen (red.)

LUFTKRIGSSKOLEN

ISBN 978-82-690521-5-2

Grafisk produksjon: Type-it AS, Trondheim

Forsidebilde: Trident Juncture 2018
Fotografer: Forsvaret - Tore Ellingsen, Hanne Hernes og Oda L. B. Iden.

Formål med skriftserien
Med Luftkrigsskolens skriftserie tar Luftkrigsskolen sikte på å synliggjøre skolens virksomhet og gjøre den mer allment tilgjengelig. I serien publiseres studier, seminarrapporter og lignende, hovedsakelig innenfor fagfeltet luftmakt og ledelse. Synspunktene som kommer til uttrykk i Luftkrigsskolens skriftserie, står for forfatternes egen regning, og er således ikke uttrykk for et offisielt syn fra Forsvarets eller Luftkrigsskolens side. Gjengivelse av innholdet i skriftserien, helt eller delvis, må kun skje med forfatternes samtykke.

Henvendelser om skriftserien kan rettes til:

Luftkrigsskolen
Persaunvegen 61
7046 Trondheim
Tlf. 73 99 54 74

Innhold

Foreword

On behalf of the Chief of the Norwegian Air Force, the Norwegian Air Force Academy is proudly hosting the annual Air Power Conference! The conference aims to place air power in a future joint operational context and a wider security policy framework.

The Air Power Conference has become a good and solid tradition. It has, for many years, become increasingly important on both a professional and a social level for those in the Armed Forces, the Air Force, and the Air Force Academy. Once again, we have chosen a topic – Multi-Domain Battle – which we think will engage, motivate, and challenge both speakers and the audience.

The Norwegian Armed Forces are in the process of considerable change, both structurally and vital elements of the education, and it seems to me that we are in need of principles and concepts that might help us discuss and relate to this development. Multi-Domain Battle might be one useful concept. The Norwegian Air Force Academy has been a key player in developing the new Norwegian Air Power Doctrine, but with the topic of this conference, we are already laying the groundwork for further developments. We must not stand idly by, believing the job to be done. Research and development will allow us to keep up with our allies and ahead of potential enemies. The rapid development of new technology and the procurement of the F-35 calls for even further development of our competence in planning, executing, and leading military operations, especially within the air power domain. I believe this conference will assist in doing just that.

The Air Power Conference has become a part of our culture. It is an indispensable arena for professional discussions. In addition, the conference provides us with the opportunity to meet colleagues and socialise.

Welcome to the Air Power Conference 2018!

Rune Gaustad
Colonel
Commandant of the Norwegian Air Force Academy

Åpning av Luftmaktseminaret

av Sjef Luftforsvaret, generalmajor Tonje Skinnarland

Statsråd, generaler, honoured guests, kjære alle deltagere på årets luftmaktseminar. Det er en stor glede for meg å kunne stå her igjen og ønske velkommen. Takk til representanten fra Luftforsvarets musikkorps, som på tradisjonelt vis åpnet med et kulturelt bidrag som er temaaktuelt.

Multi-Domain Battle: Nytt begrep med gammelt innhold?

I år ønsker jeg å utfordre med et åpent spørsmål i innledningen: *Multi-Domain Battle* – er det bare et nytt begrep med gammelt innhold, eller som britene bruker å si: Er det «old wines in new bottles»?

Den 17. desember i fjor tok de fleste av oss juleferie, mens andre opprettholdt beredskapen på våre vegne. Den samme datoen ble policyen for utviklingen mot nettverksbasert forsvar (NBF) faktisk opphevet. Grunnlaget for dette dokumentet (utgitt på begynnelsen av 2000-tallet) lyder som følger:

> Nettverksbasert forsvar betyr samhandling i nettverk i den hensikt å bruke forsvarets ressurser på en mer fleksibel og koordinert måte, og gjennom dette oppnå kraftig forbedring i effektivitet. NBF innbefatter derfor et fokusskifte fra hva hver enkelt plattform (eksempelvis fly, fartøy, stridsvogn) kan yte til hva et nettverk av plattformer kan yte. Hypotesen i NBF er at en forbedret felles situasjonsbevissthet gir forbedret samarbeid og gjennom dette oppnår en kraftig forbedring i effektivitet.

Min umiddelbare refleksjon er at NBF nå er i ferd med å bli erstattet av et begrep med mye av det samme innholdet: Multi-Domain Battle. Det handler om å ha en fellesoperativ tilnærming i alt vi gjør. Når våre helikoptre og fly opererer, gjør de det ikke for Luftforsvaret, men for Forsvaret og Norge. Når våre vakt- og sikringssoldater sikrer våre baser, gjør de det ikke for Luftforsvarets del, men for å sikre vår evne til å produsere luftmakt til bruk i fellesoperasjoner. Når vårt kontroll- og varslingssystem overvåker luftrommet, gjør det det ikke for Luftforsvarets del, men som en del av strategisk varsling for NATO og

Norge. Alt vi gjør, gjør vi for å forsvare Norge og NATO. Og alt vi gjør, gjør vi for å gjøre Norge tryggere.

Hvordan gi effekt til begrepet?

For å sikre at Multi-Domain Battle får effekt og ikke ender opp som nok et nytt trendbegrep, må vi sørge for at det blir en naturlig del av tankesettet vårt, av planverket vårt, av prosessene våre og, ikke minst, av det praktiske og operative samvirket mellom styrker på tvers av forsvarsgrener og domener.

Hvis vi skal lykkes, er vi avhengige av at utviklingen skjer nedenfra, samtidig som vi har en «top-down»-tilnærming med doktrinell og konseptuell innretning. Vi må ha fagmiljøer som finner hverandre, og som utvikler praktisk samarbeid. Gjennom slikt samarbeid vil vi så videreutvikle Forsvaret innenfor Multi-Domain Battle. Jeg er nesten fristet til å gjenopplive et gammelt «slogan» som mange av dere i lyseblått kjenner fra tidligere: «Just do it!» (innenfor de rammene vi er gitt).

Vi er nødt til å forbedre oss kontinuerlig, vi er nødt til å utfordre tradisjonell tenkning, vi er nødt til å utnytte mulighetene som ligger der. En viktig del av denne utviklingen er årlige seminarer som har til hensikt å samle personell i Forsvaret for å drive kompetanseheving og diskusjon. Gjennom dette utvikler vi kunnskap sammen og bidrar til at vi utfordrer tankesettet vårt og stimulerer den kraften som ligger i organisasjonen vår, til å samarbeide og finne praktiske løsninger. Jeg har en grunnleggende tro på at vi må utfordre hverandre for å skape utvikling og finne de beste løsningene.

Seminarers betydning for å skape utvikling

Historisk sett har luftmaktseminaret og lederskapsseminaret vært de mest kjente seminarene. For meg er det svært viktig å kunne opprettholde disse arenaene for å bidra til vår evne til kompetanseheving, kunnskapsdeling, utvikling, kulturbygging og ikke minst relasjonsbygging. I begynnelsen av året gjennomførte vi også et annet seminar som har vokst i omfang og betydning, men som er mer lukket: sjef NAOCs operative seminar. Dette seminaret er høygradert og foregår i fjellanlegget på Reitan. Årets tittel spilte på en rapport som våre norske deltagere kjenner godt: Hvordan få de fellesoperative ressursene til å møtes? Her var Multi-Domain Battle en sentral del av programmet, og jeg er glad for at vi i år klarer å skape en rød tråd fra diskusjonene i høygraderte fasiliteter til denne settingen – ugradert diskusjon og refleksjon om temaet på luftmaktseminaret.

En annen veldig positiv utvikling jeg har sett både på det operative seminaret og i salen her i dag, er mangfoldet av deltagere. Da jeg sto på talerstolen her og holdt et foredrag som ung kaptein i 1998, var det nesten bare lyseblå i salen. Nå er det veldig godt å se at det er mange deltagere fra andre forsvarsgrener – det var det også på Reitan – og ikke minst samarbeidsaktører i sivilsamfunnet og internasjonalt. Vi skaper utvikling ved å lytte til og lære av hverandre.

Forventninger til årets seminar

Bak det hele vil jeg oppfordre dere alle sammen: Dere er ikke bare tilhørere på dette seminaret. Dere er deltagere! Jeg oppfordrer dere derfor til å bidra med deres perspektiver i diskusjoner ved å stille spørsmål i plenum. Luftmaktseminaret er kjent for sin takhøyde, og den må vi sammen bidra til å opprettholde.

Avslutningsvis vil jeg takke Luftkrigsskolen ved skolesjefen og alle hans for å legge til rette et svært spennende program, som også i år er tidsaktuelt. Personlig må jeg dessverre forlate dere midtveis i seminaret. Dette er fordi vi får besøk av general Tod D. Wolters, som er COM AIRCOM i NATO og COM USAF Europe og Afrika. Han kommer til Norge for å se nærmere på Luftforsvaret, Forsvaret og Norge som NATO i nord. Det er svært viktig besøk, som falt samtidig som luftmaktseminaret.

Besøket fra COM AIRCOM har en oppbygning som tilsvarer seminarets. Det skal starte med det strategiske perspektivet gjennom FD og FST. Deretter fortsetter vi med det operasjonelle på Reitan, ved FOH og vår egen NAOC, før vi avslutter med å se nærmere på Luftforsvaret, F-35 og luftkontrollsystemet spesielt på Ørland. Jeg håper at COM AIRCOM sitter igjen med det samme som jeg håper dere sitter igjen med etter disse dagene på «Kuhaugen»: En forståelse for hvor vi er, en forståelse for hvor vi skal, og kunnskap som dere kan ta med dere hjem til der dere kommer fra, og bidra til at vi faktisk kommer dit vi skal. Målet med alt vi gjør, er å skape større operativ effekt for Forsvaret, for Norge og for NATO.

Med dette erklærer jeg årets luftmaktseminar for åpnet.

Veien videre

av Frank Bakke-Jensen

Jeg er veldig glad for at tittelen til årets seminar avsluttes med et spørsmålstegn, men jeg kan åpne med å si at jeg ikke kommer til å gi dere svaret. Men som forsvarsminister er jeg glad for at noen stiller spørsmålet. Det er skiftende tider, og det er av og til en vanskelig hverdag å navigere i. Da er vi avhengige av at noen stiller gode spørsmål, og at vi samles for å gi gode svar.

De første dagene mine som forsvarsminister fikk jeg mange innspill fra forsvarsinteresserte fra hele landet, spesielt knyttet til F-35. De var alt fra bønder på Jæren til krabbefiskere i Båtsfjord. Det sier meg to ting: at vi har en viktig diskusjon og et stort engasjement rundt Forsvaret og de store investeringene vi gjør, men også at den raske spredningen av kunnskap og debatter som vi opplever i dag, gjør hverdagen litt vanskeligere. Det er ikke en lett oppgave å henge på med oppklarende leserinnlegg i landets lokalaviser. Vi står derfor i en utfordrende posisjon når det gjelder å formidle hva som er fakta i forbindelse med endringsprosessene i Forsvaret. Derfor har jeg brukt mye tid på å reise rundt etter at jeg ble forsvarsminister. Jeg har møtt en etat med svært dedikerte, engasjerte, innsatsvillige og profesjonelle folk. Samtidig har jeg fått forståelsen av at det av og til kan være vanskelig å stå i omstillingsprosesser. Tro meg når jeg sier at jeg tar alle signalene på alvor – det må vi gjøre.

I dette innlegget skal jeg forsøke å gi et lite bilde av hvordan vi har tenkt når det gjelder planlegging, og hvordan vi ser på sikkerhetsbildet som omgir oss i dag. Jeg håper at seminaret kan fylle på med kunnskap og fakta, slik at vi nærmer oss et svar.

I mine åtte år på Stortinget har jeg vært med på å vedta to langtidsplaner. Langtidsplanen som Stortinget vedtok i 2012, sier overordnet om det strategiske bildet at «det er få tegn til endringer i det strategiske bildet som vil utløse gjennomgripende nye krav til Forsvaret i overskuelig fremtid». Fire år etter skriver vi følgende i den nye langtidsplanen: «Den sikkerhetsmessige situasjonen blir stadig mer kompleks og uforutsigbar, og endringer kan skje raskt og uten tydelig varsel.» Det sier oss litt om hvor fort situasjonen har endret seg. Det var også noe av det første jeg observerte da jeg ble NATO-parlamentariker i 2013. På det første møtet jeg var på, var det en parlamentarikerforsamling av om ikke desillusjonerte så ganske avslappede politikere. Europa var i en tilstand

av fred og fordragelighet. Kort tid etter begynte de baltiske landene, og deretter observatørlandene Sverige og Finland, å melde om urolighet. Da begynte ballen å rulle, og vi satt raskt igjen med et helt annet bilde av situasjonen.

I dag ser vi at flere fenomener inntreffer samtidig. Vi ser voksende polarisering i og mellom land. Videre ser vi anti-globalisering, anti-elite-bevegelser, anti-frihet, anti-demokrati og anti-institusjoner, politisk og religiøst motivert terrorisme og ekstremisme, massemigrasjon og økonomisk usikkerhet. Klimaendringene spiller også en viktig rolle i bildet vi ser i dag, med tanke på både mulighetene, begrensningene og sårbarhetene som endringene medfører. Dette gjør at vi må være forberedt på raske endringer. Som politiker er jeg derfor opptatt av å formidle at vi må planlegge, investere, utstyre oss og trene for det uforutsigbare og ukjente.

Norges særegne utfordringer

Norge er et langstrakt land med særegne klimatiske og geografiske forutsetninger, og vi har særegne utfordringer. Én av utfordringene er at vi som nabo i nord har en atomvåpenmakt med stormaktsambisjoner – et Russland som de siste ti årene har satset kraftig på militær modernisering og utvikling. Avanserte ubåter og oppdaterte kjernevåpen fortsetter å være i sentrum av den russiske strategien. En av Nordflåtens viktigste oppgaver er å verne om disse strategiske kapasitetene. De siste årene har vi også sett at utviklingen av russisk materiell og kompetanse styrker deres evne til å løse akkurat det oppdraget. Enten vi vil eller ikke, er vi geografisk plassert i Russlands strategiske nærområde. Det må vi ta hensyn til. Samtidig gir Russlands militære og utenrikspolitiske opptreden grunn til bekymring. Vi ser en sammenheng mellom oppbyggingen av Russlands militærmakt og landets stormaktsambisjoner. Videre har landet gjennomført destabiliserende militære operasjoner mot naboland, og Vesten ble for alvor vekket av den folkerettsstridige anneksjonen av Krim. Valget for Norge er enkelt. Men i Finnmark står jeg ofte i diskusjonen om vi er nødt til å være så tydelige overfor naboen vår, og jeg blir spurt om jeg kan fortelle til Oslo at finnmarkinger kjenner russerne bedre, og at vi tenker annerledes. Til dette pleier jeg å si at selv i Finnmark er vi ikke bare *litt* for folkeretten, men *helt* for den. Det må vi ta med i vurderingen.

Samtidig som vi ikke kan akseptere at Russland hever seg over folkeretten, er det slik at vi vil hindre videre eskalering. Norge søker samarbeid på alle plan, og vi har et stort engasjement innen folk-til-folk-samarbeid i nord. Grenseoverskridende kultur- og næringsprosjekter er et svært viktig arbeid, og vi har utvidet den visumfrie sonen i Øst-Finnmark. Videre samarbeider vi om fis-

keriforvaltning, grensevakt og kystvakt samt søk og redning. Samtidig som vi har suspendert militært samarbeid med Russland i etterkant av anneksjonen av Krim, fortsetter vi altså annet samarbeid i nord, som er et område vi alle driver kompliserte operasjoner i. For eksempel har vi direktetelefon fra Forsvarets operative hovedkvarter i Bodø (FOH) til Nordflåten, og nylig deltok medlemmer av mitt embetsverk på militære møter på embetsnivå i Moskva. Dette gjør vi for at vi skal kunne snakke sammen, nettopp for å unngå misforståelser og utilsiktet eskalering.

Hver gang jeg holder et innlegg om den sikkerhetspolitiske situasjonen, sier og mener jeg at Russland ikke er en direkte militær trussel overfor Norge i dag. Det er ingen tegn på at vi er truet. Likevel er Russland en selvhevdende stormakt som har atomvåpen, og som er utenfor det vestlige sikkerhetsfellesskapet. Og som nevnt ligger Norge geografisk plassert innenfor det strategiske nærområdet til Russland. Dette er en dimensjonerende faktor for norsk forsvars- og sikkerhetspolitikk. Det kan skje at Russland utfører handlinger andre steder i verden som de selv oppfatter som defensive, men som Norge oppfatter som offensive. Dette er et tett og komplisert bilde. Derfor er det viktig for oss å være tydelig på hvem vi er, og hvilken forsvars- og sikkerhetspolitikk vi har. Men jeg minner om at Russland i dag ikke representerer en direkte militær trussel mot Norge.

Norsk sikkerhetspolitikk og langtidsplanen

Vår sikkerhetspolitikk består av to hovedelementer. Det første er en troverdig nasjonal forsvarsevne, som jeg skal komme tilbake til senere. Det andre hovedelementet er vårt medlemskap i NATO, som har vart helt siden organisasjonens stiftelse i 1949. Etter andre verdenskrig fremsto det som åpenbart for Norge at vi ikke ville være i stand til å sørge for vår egen sikkerhet alene. Vi ble derfor medlem av NATO, som har blitt verdens mest vellykkede forsvarsallianse. Norge har klart seg svært godt med det. Gjennom NATO har vi USA og et europeisk fellesskap som garantister for norsk sikkerhet. Men det har vært en del diskusjon blant annet om byrdefordeling og ulikt innsatsnivå mellom medlemslandene. Endringene som startet i 2013, bidrar også til diskusjonen. Som en konsekvens av endringene tar medlemslandene, inkludert Norge, nå en større del av byrden. Regjeringsplattformen viser at vi jobber for å nå det vedtatte målet om at forsvarsutgiftene til Norge på sikt skal utgjøre to prosent av BNP. I den forbindelse kommer ikke jeg til å gå inn i en diskusjon om hvor vi står i dette regnskapet, hver tredje måned idet SSB kommer med nye fremskrivninger av landets BNP. Jeg kommer til å konsentrere meg om å gjen-

nomføre satsingene som står i langtidsplanen som Stortinget har vedtatt. Men Regjeringens ambisjon står fast – vi skal bevege oss mot å bruke to prosent av BNP på forsvar, i tillegg til å løse de andre kravene vi blir målt etter. Dette inkluderer at vi har relevante kapasiteter, at investeringsgraden er over 20 prosent, og at vi deltar i operasjoner hvor NATO har behov for våre kapasiteter.

Basepolitikken står fast

Som følge av endringene i NATO i 2013 har det nordlige Atlanterhavet og nordområdene fått mer oppmerksomhet. I fjor høst ble det besluttet at NATO skal opprette en stående maritim kommando for å sikre den transatlantiske forbindelsen, og et planverk og en kommandostruktur som passer til dette. Dette har vært et norsk ønskemål lenge og innebærer at NATO går tilbake til det gamle oppdraget. Det er vi veldig fornøyd med. I tillegg har Norge, gitt den geografiske beliggenheten og vårt store naboland i øst, pålagt seg selv restriksjoner hva gjelder vårt NATO-medlemskap. Det betyr at vi ikke skal gjennomføre allierte flyvninger øst for 24. lengdegrad, og at vi ikke skal ha fremmede baser på norsk jord. Men det innebærer også at vi må kompensere med mer alliert trening. Hovedgrunnen til dette er at i tilfelle Norge behøver hjelp, er det viktig at vi kjenner dem og de kjenner oss. Vi må ha øvd med dem, og de må stole på oss. Derfor øver vi mye i Norge, og vi øver operativt med våre allierte i utlandet. Alliert trening skal vi ha, og våre allierte har vært her i mange tiår allerede. Når aktiviteten tar seg opp rundt Atlanterhavet og Nord-Europa, blir det mer alliert trening. Likevel er det ikke sånn at dette er et brudd med den tidligere basepolitikken, og det er det to grunner til. For det første er det ikke tilfellet at vi opererer med fremmede baser på norsk jord. For det andre er det klart at basepolitikken er et norsk anliggende, og enhver sittende regjering har spørsmålet om hvordan vi skal forvalte denne politikken, til vurdering. I dag har vi den mengden alliert trening som vi mener er hensiktsmessig, gitt den situasjonen vi står i i dag.

Nordområdene er vårt viktigste ansvarsområde. Forsvarets bidrag til nordområdepolitikken er blant annet overvåkning, suverenitetshevdelse og tilstedeværelse i nord. Vi trenger god situasjonsforståelse for å unngå de tidligere nevnte misforståelsene. Når sikkerhetssituasjonen blir vanskeligere, må vi seile, fly og være mer til stede i nord, og det gjør vi nå. Nesten halvparten av marinens aktivitet foregår i nordområdene. Vi skal etablere en felles landkommando i Finnmark, som skal lede både Hærens og Heimevernets styrker. Hæren tas tilbake til Porsanger, hvor det skal opprettes en ny kavaleribataljon, og vi skal styrke grensevakten. I det hele øker vi Forsvarets tilstedeværelse og aktivi-

tet i nordområdene, fordi sikkerhetssituasjonen tilsier det. I tillegg ivaretar vi NATOs interesser i nord. Norge er NATO i nord.

Teknologiske omstillinger

Teknologi er også en dimensjonerende faktor for endringer i sikkerhetspolitikken. Under den kalde krigen var Forsvarets teknologi den ypperste. Da krigen var ferdig, satt Vesten igjen med et enormt teknologisk forsprang. Slik er det ikke lenger. For det første er det mange land og verdensdeler som har kommet seg opp på samme teknologiske nivå som det Vesten er på. For det andre kan vi nesten ikke lenger skille mellom militær og sivil teknologi. Det betyr at mange flere kan være med i et teknologisk kappløp. Det gir stadig flere anledning til å ta i bruk avansert teknologi til militære formål. En spesiell utfordring er langtrekkende konvensjonelle presisjonsvåpen, og det er en utfordring som går begge veier. Slike våpen gjør det mulig å ramme en motstander på kort varsel uten å utsette eget personell for fare. Presisjonen gjør det også mulig å ta ut strategiske mål med mindre fare for sivile tap. Det faktumet kan raskt bidra til å senke terskelen for å bruke den typen våpen, og det må vi ta med i vurderingen.

Et annet viktig poeng er at både NATO og Russland opplever denne typen endringer i trusselbildet, og endringene er synlige på mange måter. I langtidsplanen tas dette høyde for så godt det lar seg gjøre, ved at det legges opp til at vi skal utdanne nytt personell og kjøpe nye kapasiteter. I tillegg skifter vi systemer. Ved bytte av systemer kan forsvarsevnen midlertidig reduseres, noe som er en utfordring for personellet vårt. Likevel er det nødvendig å bytte kapasiteter, og nå bytter vi ut mye. Dette tar vi hensyn til i omstillingen fremover.

Hvordan planlegges det for fremtiden?

Langtidsplanen som ble vedtatt i 2016, gjelder til vi har vedtatt en ny plan. Det fine med hvordan vi planlegger i Forsvaret, er at vi har en langtidsplan som tenker 20 år fremover, mens vi budsjettmessig tenker fire år fremover. Etter cirka fire år rulleres planen. Det gjøres for at vi skal være sikre på at vi klarer å holde oversikt over om vi gjør som planlagt, og for å skape rom for endringer ved behov. Ved slike justeringer forpliktes politikerne på nytt, og det er dermed en god metode for å operasjonalisere et planverk. Ved langtidsplanen fra 2016 var det så mange spørsmål knyttet til landmakten at det måtte utredes ekstra, noe som førte til at vi vedtok en landmaktproposisjon i 2017. Dette er noe av det viktigste jeg forteller når jeg reiser rundt – at disse to vedtakene skal føre til ett

dokument. Langtidsplanen kan ikke justeres uten at det går utover landmaktproposisjonen, og vice versa. Men for øyeblikket er man nødt til å lese begge dokumentene for å få hele bildet.

Et sentralt element i planen er anskaffelsen av nye kapasiteter med strategisk betydning. Dette inkluderer maritime patruljefly og fire nye ubåter i samarbeid med Tyskland. F-35, en formidabel kapasitet, er i ferd med å innfases. Etter hvert vil vi få et av de mest slagkraftige luftforsvarene i Nord-Europa. For å kunne nyttiggjøre oss disse kapasitetene er hele Forsvaret i gang med å utvikle kompetanse og konsepter for å bruke flyene riktig. Nye våpensystemer, teknologisk utvikling og endring i det sikkerhetspolitiske landskapet gjør at langtidsplanleggingen er en dynamisk prosess. Samtidig skal vedtakene om bevilgninger, prioriteringer og gjennomføring følges opp. Balansen er viktig, og hvis noe er i ubalanse, må det justeres. Hvis vi ikke gjøre dette, risikerer vi en bråstans.

F-35 er et formidabelt femtegenerasjons kampfly som vil være hjertet i fremtidens femtegenerasjons luftforsvar. Samtidig vet vi at hvis vi har et femtegenerasjons kampfly, må vi utvikle femtegenerasjons baser og femtegenerasjons luftvern. Med andre ord har vi store utfordringer foran oss, selv om vi har kjøpt nye og svært gode fly.

Foruten Luftforsvaret har vi de andre tradisjonelle domenene: sjø og land. Noe av det viktigste vi må venne oss til fremover, er at vi ikke kan tenke på de ulike domenene som isolerte. Videre har vi fått cyberdomenet, som blir stadig viktigere. I tillegg har vi verdensrommet, det femte domenet. I dette domenet ligger satellittene, som spiller en stor rolle for vår evne til å kommunisere og å se ting. Domenebegrepet blir således utvidet betraktelig, og et sentralt poeng er at disse domenene blir stadig mer sammenvevd. I tillegg blir disse domenene i økende grad knyttet sammen med det sivile samfunn, institusjoner og teknologi, og det betyr at vi er avhengige av å utvikle et nytt konsept med tiden.

Luftforsvarets historie gir oss et godt bilde på slike endringer. Over flere tusen år har vi vært begrenset til domenene sjø og land. Men spesielt i tiden under og etter andre verdenskrig har fly og Luftforsvaret etablert seg og blitt styrende for hvordan krig og forsvar gjennomføres. I løpet av førti–femti år ble et nytt dominerende domene opprettet. Det vil ikke bli mindre betydningsfullt å koble de tre tradisjonelle domenene med cyber- og romdomenene i fremtiden, og utviklingen vil skje uhorvelig raskt. Dette øker kompleksiteten, og derfor er det flott at spørsmålet «Hva er et multidomene?» stilles. Vi kommer til å bruke mye tankekraft og de beste folkene vi har, for å gi et svar på dette i fremtiden. I forbindelse med dette har jeg overhørt både at dette kan bli for stort for et lite land, og at vi er nødt til å fylle begrepet med vår forståelse og vårt innhold. Derfor er vi i gang med flere tunge ting. Utdanningsreformen

gjør at vi utdanner andre typer offiserer, og vi innfører et spesialistkorps fordi vi behøver mer spisset kunnskap i møte med den nye kompleksiteten. Vi vil også se et større innslag av sivile i Forsvaret, på arenaer vi tidligere har tenkt at vi ikke kom til å se sivile. I tillegg rendyrkes og spisses offisersrollen.

Et forsvar i omstilling

Vi er i gang med å implementere en langtidsplan og en landmaktproposisjon, og vi har et nytt sikkerhetsbilde som endrer seg nærmest ukentlig. Forsvaret moderniseres rundt F-35, som krever mye av Luftforsvaret. Store oppgaver knyttet til P-8, helikopter og nytt kampfly venter. Jeg har sagt at vi skal stå på for å ivareta personalet i denne perioden, som ikke kommer til å bli enkel. Det må tas på alvor. Jeg vet at dette er utfordrende, men jeg har tillit til at dere lykkes.

I tillegg er det tydelig at Luftforsvaret er på ballen nå som dere har avholdt tre seminarer hvor det sees på henholdsvis spesialistrollen, offisersrollen og nå hva som skal fylle begrepet «Multi-Domain». Dette er bra. Politikere skal levere et målbilde, og med det som utgangspunkt skal dere skape kompetansen, konseptene og teoriene som får alle delene til å fungere sammen som en helhet. Takk for at disse fremoverlente seminarene holdes. Ettertanke er en av de viktigste egenskapene når det gjelder evnen til omstilling og det å tenke nytt. For å se hva vi kan være, må vi vite hvor vi kom fra, og hvorfor vi har kommet hit vi er i dag. Vi behøver et femtegenerasjons luftforsvar i et moderne og relevant forsvar, og tusen takk for deres innsats for å nå det målet.

The absence of a global order

by Carl Bildt

From a historical perspective, there has always been either global order or global disorder, and a balance between them. For example, the period marked by the Hanseatic League has been important both for Sweden and Norway. Looking back at the period, enquiring as to what it really was, we see that it was a period of commerce, interaction, and relative peace because of a balance of power between the dominating powers. Furthermore, this period was made possible because of advances in shipping technology, whereby the ships could carry larger loads, and a common understanding of law; not necessarily international law, in the sense that it is interpreted today, but commercial laws which applied within the cities of the Hanseatic League, stretching from Russia, to the Nordic Countries, Flanders, and Great Britain. This enabled a prolonged period of prosperity and relative stability. Since then, order and disorder has gone back and forth, such as the Peace of Westphalia in 1648, the Peace of Utrecht in 1713, and the Peace of Vienna in 1815, the attempt of constructing a world order after the First World War. Following this are the efforts made in the modern age.

The modern global order

I think that the modern search for global order can be traced back to August 1941. That year, there was a meeting between the – up until this point – dominating global power, Great Britain, and the rising global power, the United States of America. The Axis powers were still growing in importance, and Stalingrad had not yet taken place. Working jointly, they set up the Atlantic Charter, not only defining the aims of that particular war, but also the outlines of the global order that they ought to install if they were victorious. As we know, they did win the war, and they did set up a global order. The United Nations was created, together with a network of different organisations such as Bretton Woods, the World Bank, and the International Monetary Fund. Global organisations were created in all the different areas of international governance. This has turned out to be referred to as the liberal global order. It ensured unprecedented development and prosperity to large parts of the world, including the

Atlantic allies, in addition to ensuring the reconstruction and reconsolidation of Germany and Japan. Although there was not a complete absence of war, the liberal global order ensured relative peace from a longer historical perspective. Furthermore, a quarter of a century ago, the Soviet Empire collapsed. The bipolar world was replaced by what is sometimes referred to as a 'unipolar world', a world with the United States as the supremely dominant power, also described as the end of history, referring to a closure of global and ideological battles.

However, even at that time, I think it was obvious that that situation would not last forever; things in history never last forever. The big shift has happened gradually, but the turning point, as I see it, was probably around 2008. Having been a tumultuous few years, a number of things happened: the political battles of the future of Kosovo; the West's recognition of the extent of Russia's military might in its vicinity being lower than we thought, given the wars between Russia and Georgia; the collapse of Lehman Brothers, followed by a deep financial crisis, and a near-death experience for the process of financial and economic globalisation, a crisis which we managed to get out of due to an unprecedented level of international cooperation. However, one of the things that has happened since is that Russia decided to accelerate its military modernisation, which hadn't happened before. For example, during the 15 years prior to 2008, more modern fighter aircrafts had been delivered to the Swedish air force than to the Russian air force. In these 15 years, we've seen a very rapid increase in Russian military spending, and an increasing preparedness to use military power for different political ends. Thus, for a number of reasons, we find ourselves in a new situation.

To sum up the moment, we see geopolitics challenging the forces of globalisation. Since February of 2015, we've seen 10,000 people killed in the battle of Eastern Ukraine. Secondly, the politics of identity is replacing ideology throughout the Western world; in other words, the politics of fear is replacing the politics of hope. We see this not only when it comes to so-called Islamic State (ISIS), but in our own countries as well. For example, what is currently happening in the United States, with President Donald Trump's rhetoric of 'making America great again'. Ronald Reagan would have said that we ought to make America great, moving forwards – which is a contrast to Trump's emphasis on 'again'. This is nostalgia for the past, the sentiment that the country was better before. We see this kind of politics in one country after another. Politics of fear and identity has replaced the politics of ideology. Lastly, we are in the end of the industrial era, finding ourselves in the beginning of the digital era, which has only faintly begun. If we were to compare this with the age in which

we went from the agricultural to the industrial era, we would probably find ourselves in the period when the second generation of the steam engine came. Those who were wondering about the marvels of the second generation of the steam engine had no clue what was to come in the next 200 years. Similarly, we know very little of what lies ahead of us in the digital era, in spite of everything that has happened since this particular era began. The forces of history are changing our world.

A shift in U.S. perceptions

If we look at the different actors on the global stage, it is natural to start with the United States. Although it is the hitherto dominant power, it has begun to question its own policies. The National Security Strategy of the United States of America released in December 2017 which, after some internal turmoil, they managed to produce, is an interesting document; it is very different from the documents we've previously seen coming from Washington. The key difference is that every single previous national strategy of the US has emphasised the search for a global order of some sort – a liberal global order, an international global order, or an American dominated global order. However, in this recent document, the phrasing 'global order' is not mentioned. Instead, it is based upon the view that '*peace*, *security*, *and prosperity depend on strong*, *sovereign nations that respect their citizens at home and cooperate to advance peace abroad*'. In addition, it can be understood that the global order is perceived not to have had a positive influence on the United States, but rather a negative one, and that the global order needs to be revised in different ways[1]. Furthermore, the United States is in a competition with other states[2]. If there's any vision of the global order in the document, that is it. This may sound good from Washington's point of view, but it is somewhat different from a European point of view. From the European point of view, sovereign states competing with each other without any overriding order is what we have seen in Europe for the last few centuries, and that which has produced the wars. This has also led to the European search for some sort of a global order. This American shift in perceptions

1 '*We stood by while countries exploited the international institutions we helped to build. They subsidised their industries, forced technology transfers, and distorted markets*'.

2 '*These competitions require the United States to rethink the policies of the past two decades based on the assumption that engagement with rivals and their inclusion in international institutions and global commerce would turn them into benign actors and trustworthy partners. For the most part, this premise turned out to be false*'.

is important. The National Defense Strategy, which was released somewhat later, is also important. It is interesting in the sense that the War on Terror is now no longer dominating[3]. The primary U.S. concern has shifted to inter-state strategic competition, signalling that geopolitics is back in business, and the re-emergence of long-term strategic competition with China and Russia[4]. (However, in this particular document published by the Pentagon, the wording 'international order' is present. There is a different tone from the White House compared to the Pentagon).

The Rise of China

Something huge that has happened during the last decades is the rise of China. When I started in politics, China was a poor dictatorship. To put it briefly, it was completely isolated from the world, and did not exist on the international markets. Mildly speaking, that is no longer the case; now it is a rising, confident power. The relationship between the United States and China is marked by that of a still dominant power and a rapidly rising power. What happens between them will decide much of what happens in the world in the years to come.

When President Donald Trump was allowed to visit and served dinner within Beijing's Forbidden City, the Russians were downright scared. The reason being that this honour has never been bestowed upon any Soviet or Russian leader. To the Chinese, Russia is 'there', but it is there among other countries. However, it is its relationship to the United States that counts. This is a clear sign of the priorities of a confident China. In a speech to the National Congress of the Communist Party of China, President Xi Jinping stated that 'the military is there to fight wars'. Military power, which has previously been fairly low on the list of Chinese priorities, is gradually rising. Furthermore, the way the Chinese portray this to the public is quite different now from before. Step-by-step, they are building impressive military competence, to which civilian tech-

3 *'Today, we are emerging from a period of strategic atrophy, aware that our competitive military advantage has been eroding. We are facing increased global disorder, characterised by the decline in the long-standing rules-based international order – creating a security environment more complex and volatile than any we have experienced in recent memory. Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security'.*

4 *'The central challenge to U.S. prosperity and security is the re-emergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers. It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model – gaining veto authority over other nations' economic, diplomatic, and security decisions'.*

nology is of enormous importance. For example, at the moment, the Chinese are investing more in artificial intelligence than all of the European nations combined.

In my opinion, the rise of China is the single most important thing that we need to know about the security of Europe in the time ahead. Since the Second World War, the security of Europe has been a function of the Atlantic alliance and other associated relationships. Europe, having gradually built itself up – including in a military capacity – has been dependent upon the United States for key resources, such as nuclear, reinforcements, intelligence, command and control, and so on. Now, however, we see a change in the relative size of the military spending of China and the United States. In 2014, U.S. military spending constituted roughly 45 percent of all the military spending in the world. China is substantially behind. However, by present trends, Chinese military spending by 2035 will start to be the same level as U.S. spending; this will lead to an increasing portion of U.S. attention and resources being rebalanced towards meeting the rise of China if it wants to be committed to the stability of East-Asia, which is still the most dynamic part of the global economy. In that particular respect, the Americans are left without much of a choice. Even today, in the event of a major conflict on the Korean peninsula in which the U.S. would have to reinforce their current standing forces in the area, the U.S. would find it difficult to handle a simultaneous situation in our part of the world. Regarding the security of Europe, this changes the equation. Even though something in the long-term could make the situation less insecure, such as a collapse of the Chinese economy, I would not bet the security of our nations on it.

The case of Russia

In a speech held by the Russian president Vladimir Putin at the Valdai Conference in 2014, he was quoted saying '*Today's discussion took place under the theme: New rules or a Game without Rules*'. If we think about what he actually says, it meant that he does not accept the rules as they are. Either we change the rules of the game, or we play without rules – a fairly explicit statement. He then continued to present an inept interpretation of history: "*First of all, changes in the world order – and what we are seeing today are events on this scale – have usually been accompanied by if not global war and conflict, then by chains of intensive local-level conflicts*'. Whether that interpretation of history is correct or not is a separate issue. But the important fact is that this is the belief of the president of the Russian Federation. This, of course, will guide his actions in different

respects. And as we know, this is somewhat easier said than done. Putin made a statement some years ago, stating that the collapse of the Soviet Union was the biggest geopolitical catastrophe of the 20th century. However, when historians look back at this period, I think the loss of Ukraine will be a major disaster from Russia's point of view. You can lose Germany, Georgia, Bulgaria, and Estonia, but Ukraine is different. Furthermore, invading countries is historically a very bad way to make friends. In doing this, he has created a Ukraine that is more united and less friendly towards Russia than has ever been the case throughout history. The consequences of this – and what will be Putin's next step with the military means at his disposal – remain unknown. However, we have every reason to be concerned.

Europe's choices

Where does all this leave Europe and the European Union (EU)? The first time the EU laid down a security strategy in 2003, it started with a famous phrase stating that "*Europe had never been as peaceful, prosperous, and stable as it is now*'. In 2003, this was roughly true. This is clearly not true today. A couple of years ago, the European Union's Foreign and Security Policy emphasised in its Global strategy document "*A shared Vision, Common Action: A Stronger Europe*' the disorderly and dangerous world that we're currently facing. This is from the European point of view, given that Europeans naturally want to promote a global order based on rules. Europe can't dominate the world and is dependent on a world in which everyone abides to the rules[5]. However, the EU puts an increasing emphasis on security and defence, though widely defined[6]. The EU is not NATO or a military alliance, but you might ask whether it has become a security alliance in terms of how the EU states that it will enhance the efforts on defence, the cyber domain, counterterrorism, energy, and strategic communications. Often in close cooperation with NATO, the EU is putting increasing efforts into these widely defined security related issues, ranging from migration, terrorism, the cyber domain, and hybrid warfare. In certain areas of the global order, however, the EU is a very strong and important actor, such as in

5 *'The EU will promote a rules-based global order. We have an interest in promoting agreed rules to provide global public goods and contribute to a peaceful and sustainable world. The EU will promote a rules-based global order with multilateralism as its key principle, and the United Nations at its core'.*

6 *'We will enhance our efforts on defence, the cyber domain, counterterrorism, energy, and strategic communications. Member States must translate their commitments to mutual assistance and solidarity enshrined in the Treaties into action'.*

the order of global trade, interaction, and the economic sphere. But recently, the United States backed out of the Transatlantic Trade and Investment Partnership (TTIP), in addition to questioning every single trade agreement the U.S. has. This has led the EU to conclude trade agreements at an unprecedented high pace, such as with Canada, South Korea, Mexico, and Japan. After all, the EU is the largest trading partner for 90 countries around the world, China being a competitor. In that sense, the EU plays a role in upholding, defending, and promoting a global order. Europe, however, being situated where it is raises areas of concern. Surrounding Europe is an arc of instability and dysfunctionality. We cannot predict what will happen in the years to come. The only thing I can predict with certainty is that the situation is not going to be as it is today. The combination of surrounding regimes' lack of legitimacy, the politics of identity, and unresolved issues mean that the instability that we have been seeing in these regions is bound to increase. Regions with instability and wars include, among others, Afghanistan, Yemen, the Sanai peninsula, Iraq, Syria, and Libya. Even small nations, such as Norway and Sweden, are currently forced into foreign self-interest, conducting stability operations in our periphery that has areas of instability with which it is likely to remain for a long time to come. This is different from the geostrategic battles between the Russians, the Chinese, and the Americans, which are fought on 'Old Power' terms. Although these conflicts are often fought with rudimentary weapons, they can still force millions of people to flee, cause state collapse, and help spread ideologies of hatred and evil even deeper into our own societies.

What, then, can we do? At the moment, Europe can, in different ways, try to preserve what is left of the global order. For example, the fundamentally important alliance-relationships such as NATO and others, in addition to The Paris Climate Agreement. We need to preserve the extremely important Iran Nuclear Agreement, which prevented a war that would have been devastating, and on a very large scale. Although the agreement does not solve everything, preventing a war is not necessarily a bad thing. Furthermore, we need to continue to fund the United Nations, which Norway is heavily engaged with when it comes to the Middle East and Palestine. We need to continue the focus on nuclear arms. Recently, the Strategic Arms Reduction Treaty came into effect, forcing the Americans and Russians down to 1,550 deployed strategic warheads each, down from around 25,000 each some time ago. However, the U.S. and Russian modernisations of their nuclear arsenal, the North Korean situation, and other significant questions might lead to pressure on this agreement and strategic nuclear uncertainty might return if we are not careful. At the moment, there is a distinct lack of dialogue between the major nuclear powers. And as

mentioned, trade issues are extremely important, given that it is trade that links countries together.

There are other reasons for which we have a fundamental interest in a global order and a rules-based world. What happens in the Arctic in the future? It is a huge area, which is slowly opening up due to global warming. There is a risk of strategic competition, and if that happens without rules, it could be dangerous. Norway, Sweden, and other countries are firmly committed to the international laws governing the sea. Norway has also recently sorted out its border delimitation issues with Russia, which was done in one of the 'softer' periods of relations with Russia. Currently on the table are major issues regarding the future delimitation of the Arctic continental shelf. The Svalbard Treaty, among other treaties in the region, is also of importance. We need to safeguard every aspect of the existing global order in order to prevent strategic competition in the Arctic from becoming dangerous for everyone involved.

The Cyber domain

At the moment, the cyber domain worries me the most. This is because it is the domain in which things are currently happening in the world today. Global trade has been fairly flat in recent years, but global cyber flow has increased 45 times in the last five years. Within five years, 95 percent of the world's population will be connected to mobile broadband networks with the same as or better capacity than we have in Europe today. This is an enormous flow of data and information, of both good and evil material. In reality, nothing of this flow is truly regulated by international law. Some efforts are underway, such as the EU's General Data Protection Regulation (GDPR), which will be a major factor when it comes to the rules regarding privacy on a global scale. But efforts within the United Nations, to go beyond simply saying that the rules of law apply in cyberspace as well, have not gone anywhere. If this does not happen, there is a risk of the present proliferation of offensive cyber capabilities. Cyber-weapons are more dangerous than nuclear weapons, given that nuclear weapons are easier to control. If cyber-weapons, although fairly difficult to design, are ever lost, they will quickly spread. When sending cyber-weapons away, they do not explode, and may be picked up and redeployed by anyone. An example is the 'Wanna Cry' virus which nearly brought down the U.K. National Health System. The virus was developed by the U.S. National Security Agency (NSA), but was either leaked or stolen, only to evidently end up with the North Koreans. They redesigned it slightly and happened to deploy it in a way the North Koreans didn't understand. It caused chaos in countries all over the

world. This is dangerous stuff, which needs to be brought under control, and against which we need to build defence.

Conclusion

In Henry Kissinger's new book, *The World Order*, he states that "*Our age is insistently, at times almost desperately, in pursuit of a concept of world order. Chaos threatens side by side with unprecedented interdependence*'. We are extremely dependent upon each other, but the order is eroding. There is a risk of chaos, with all that it entails. He asks a rather chilling question: "*Are we facing a period in which forces beyond the restraints of any order determine the future?*'. This, we do not know – but it is the question. Policies of different sorts, be they of defence, foreign, European, or global, should be pursued with the aim of preventing this from happening.

The global shift of power[1] – military consequences[2]

by Øystein Tunsjø

Introduction

The global power shift during the last decade marks that an era of unprecedented unipolarity has ended. Against conventional knowledge that the international system is returning to multipolarity, this paper argues that the international system has returned to *bipolarity*. Examining the international system from a bipolar perspective, with the United States and China as the two poles or superpowers, provides a different starting point for explaining and forecasting how the relative rise of China is altering the nature and intensity of security competition in Asia and world affairs. No other studies within the field of international relations and security studies have thoroughly examined US–China relations, the most important bilateral relationship of our time, from a bipolarity perspective.

The paper challenges the mainstream view found in the works of, among others, Henry Kissinger, Graham Allison at Harvard University, and John J. Mearsheimer at Chicago University, that US-China relations are destined for war and tragedy based on great power rivalry and power transition during previous multipolar systems. By using the return of bipolarity as a starting point, I discuss whether the new bipolar system will resemble the Cold War stability of the previous bipolar system. The argument is that a bipolar system concentrated in East Asia with superpower rivalry largely in the maritime domain, instead of in Europe, and with the main rivalry on land, will be relatively more unstable, and the risk of limited war higher than during the previous bipolar

1 This section draws on Øystein Tunsjø, *The Return of Bipolarity in World Politics: China, the United States and Geostructural Realism* (New York: Columbia University Press, 2018) https://cup.columbia.edu/book/the-return-of-bipolarity-in-world-politics/9780231176545

2 This section draws on Øystein Tunsjø, 'China's Rise and Strategic Adjustment in East Asia and Europe,' *IFS Insight*, 1/2018 https://forsvaret.no/ifs/Publikasjoner/ifs-insights-kronologisk-(2010-)/china-s-rise-and-strategic-adjustments-in-asia-and-europe

system. While this conclusion is similar to Allison's *Destined for War* thesis and Mearsheimer's *Tragedy of Great Power Politics* assumptions, we should arrive at such an argument about the most important state relationship of our time for the right reasons.

Divided into four parts, the paper first presents why the international system has returned to bipolarity. The second part emphasises why polarity matters in international affairs. The third part draws on geostructural realism, and compares the contemporary bipolar system with the previous bipolar system in the 20th century. The fourth part examines some military consequences from the re-emergence of bipolarity.

Measuring global power shifts

There is broad consensus within the field of international politics that whether the international system is multipolar, bipolar, or unipolar shapes state behaviour and conditions the possibility of peace and stability. According to Kenneth Waltz's seminal study, *Theory of International Politics*, poles and polarity within the international state system can be defined according to how the great powers 'score on *all* of the following items: size of the population and territory, resource endowment, economic capability, military strength, political stability and competence.' By drawing on Waltz's definition for measuring and counting poles in the international system, China's current combined capabilities place it in the top ranking with the United States despite the fact that there is asymmetry and no power parity between the US and China. It is important to remember that the Soviet Union never measured up to the United States' combined capabilities during the previous bipolar system. Despite the asymmetric power relations, the international system was defined as bipolar for roughly forty years.

Moreover, other contemporary great powers do not measure up to China's combined capacity. China is catching up with the United States faster than any other great power is catching up with China. A bipolar system is a system in which no third power can challenge the top two. The power gap between China and the third ranking power has become so great that we can now start to think of the international system as bipolar.

It was not the asymmetric power relationship between the United States and the Soviet Union at the start of the previous bipolar system that preoccupied observers the most when defining the international system in the post-World War Two period. Instead, Morgenthau's classic study *Politics Among Nations*, emphasised that the international system had shifted from a multipolar to a

bipolar one in the aftermath of the Second World War because the United States and the Soviet Union, 'in view of their enormous superiority over the power next in rank [Great Britain], deserved to be called superpowers.' In sum, three factors explain why the contemporary international system is bipolar: 1) The narrowing power gap between China and the U.S., 2) the widening power gap between China and any third ranking power, and 3) the similar distribution of capabilities between the origins of the contemporary bipolar international system and the previous bipolar system.

Why polarity matters

Determining polarity is important as it allows for predictions about the prospects for stability and patterns of state behaviour depending on whether the international system is multipolar, bipolar, or unipolar.

Few factors have shaped Norway's foreign policy and defence posture more than polarity. During the multipolar system up until World War Two, Norway sought isolation from great power politics and neutrality. The bipolar system that emerged in the post-World War Two period, which compelled Norway to choose sides between the two superpowers, pushed Norway to enter the North Atlantic Treaty, and sparked the development of a national defence centred on mobilisation and total defence. The collapse of the Soviet Union and the unipolar post-Cold War era presented Norway with new opportunities. Norway restructured its armed forces in order to contribute towards wars in the Balkans, Afghanistan, and Libya, policies and actions that were simply unthinkable and impossible to carry out during the previous bipolar system. A new bipolar system will not resemble the past, but will shape Norway's foreign and defence policy in new directions.

From a theoretical point of departure, polarity, or how power is distributed among the top-ranking states in the international system, is used by structural realists to explain and predict superpowers' or great powers' pattern of behaviour (balancing) and stability (risk of war). Waltz's core argument was that balancing differs between bipolar and multipolar systems, and that a multipolar system is more unstable than a bipolar system. Great power rivalry and alliance dynamics contributed to two world wars under multipolar systems, but the bipolar system was characterised more by the superpowers' internal balancing, and remained a cold war, or what the historian John Lewis Gaddis called 'a long peace'.

However, Waltz never compared the relative stability of two bipolar systems. We cannot use structural realism to explain and predict whether contemporary

US–China rivalry will resemble US–USSR rivalry during the previous bipolar system. Equally important, Waltz's structural realist theory cannot explain or predict whether a bipolar system in the 20th century will be more or less stable than a bipolar system in the 21st century.

In the current debate, scholars and policymakers are grappling with the following two overarching questions: What will US–China rivalry in the 21st century look like? Will China rise peacefully? These questions are of utmost importance today. If the current international system is returning to bipolarity and not multipolarity, then this will influence the way we answer these two important questions. Some contend that US–China relations are ripe for conflict and tragedy. Their analogies and assumptions about rivalry and the likelihood of war are drawn from multipolar systems in the past, and are based on a contemporary transition to multipolarity. However, with the current international system returning to bipolarity, we might expect another period of the 'long peace' that characterises the previous bipolar system. The current transition to a new bipolar system matters if we seek to explain and understand important developments in international politics.

Geostructural realism – accounting for the effects of a new bipolar system

My recent book *The Return of Bipolarity in World Politics* is the first study that compares states' balancing behaviour, and examines the relative stability between two bipolar systems. It refines Waltz's structural realist theory, and develops a new geostructural realist theory. Geostructural realism contends that, although it is important whether the international system is bipolar or has some other structure, stability and balancing are heavily affected by geopolitics and the way in which geography affects the two superpowers and their relationship.

The superpowers' patterns of behaviour of the previous bipolar system in the 20th century were stability, strong balancing, and strong competition and rivalry at the periphery. The new bipolar system is characterised by: 1) instability and a relatively higher risk of limited war between the two superpowers, 2) moderate balancing instead of arms racing and strong balancing, and 3) limited competition and rivalry at the periphery in contrast to strong rivalry and proxy wars during the previous bipolar system. Geostructural realism can explain why the superpowers' pattern of behaviour and stability differs in the new bipolar system.

Geostructural realism maintains that there is a relatively higher risk of limited war in a US–China bipolar system than in the previous US–Soviet

bipolar system because superpower rivalry in the 21st century is mainly at sea. However, since there are water barriers and buffer states between the two superpowers and their allies in the new bipolar system concentrated on East Asia, in contrast to the superpower confrontation on the land mass in Europe during the previous bipolar system, geopolitics impedes and defers strong balancing and arms racing in the contemporary bipolar system. Finally, because the two new superpowers are mainly rivals at sea in East Asia rather than on land, the superpowers in the new bipolar era are likely to be preoccupied with challenging status quo and spheres of influence at the new power centre in East Asia, and less involved in rivalry and proxy wars globally.

Waltz only noted anarchy and the distribution of capabilities as systemic factors in his theory, but geopolitics has important regional and systemic effects. Since Waltz's theory disregarded the importance of geopolitics, the explanatory power of his theory proved too limited. Moreover, since Waltz could not compare and contrast bipolar systems, his neorealist theory was too Eurocentric.

The importance of improving our understanding of how the superpowers behave in a new bipolar system and how systemic constraints will compel and constrain state behaviour is, without exaggeration, of utmost importance. If the risk of war is higher at the centre in East Asia in the new US–China bipolar system than the previous bipolar system risked war emerging from US-Soviet rivalry in Europe, then it is useful to know more about the risk factors so that these effects can potentially be mitigated. If the patterns of behaviour in the new bipolar system of the 21st century are not similar to the strong balancing and confrontation that characterised the Cold War of the previous bipolar system in the 20th century, then it is important to know why.

Military consequences

The new bipolar system is not just important in responding to a few pivotal questions in international politics, namely balancing, stability, and states' room for manoeuvre; the return of bipolarity is likely to shape a number of military developments. The contemporary rise of China suggests that the balance of power in the United States' two flanking regions is only challenged in East Asia.

China's GDP and defence spending is roughly equal to the combined GDP and defence spending of all the East Asian states, including Russia and India. By way of contrast, the US' allies can maintain a balance of power in Europe. Because China is more powerful than all other states combined within its

region, the US is likely to become more preoccupied with East Asia, and increasingly shift more of its resources and capabilities towards this region.

This geopolitical shift is likely to affect NATO's ambitions for collective defence in Europe, and shape its new maritime strategy. US–China rivalry will primarily be in the maritime domain. In 2016, the People's Liberation Army Navy commissioned 18 ships with a total displacement of 150,000 tons, roughly half of the overall displacement of the British Royal Navy that year. Balancing China's regional ambitions in maritime East Asia requires a strong forward US air and naval presence.

The primary challenge from Russia is on the ground in Europe. While its naval capabilities pose a potential threat, this remains secondary to the continental theatre. Thus, the US army might sustain a light footprint in Europe, but US naval and air forces are likely to be concentrated in the Asia-Pacific. Naval and air assets can move between regions, but ships and aeroplanes can only be in one place at one time. The US is unlikely to abandon Europe or NATO, but global power shifts suggest that a forward presence to counter future Russia's activities in the Northern Atlantic and the High North is likely to be, at best, a secondary priority for the US Navy.

Since contemporary Russia is not the mighty Soviet Union that once threatened Western Europe and maritime lines of communications in the Atlantic, the northern region is less strategically vital to the US and NATO today. But since China has emerged as the only peer competitor to the US, and the US is shifting its naval capabilities towards the Asia-Pacific, a revitalised Russian Northern Fleet is provided with an opportunity to assert its interests in the High North and the Northern Atlantic. If Russia's military wishes to control the Barents Sea and develop strong anti-access and area denial capabilities in the North Atlantic, current technological developments – especially long-range, precision guided ballistic and cruise missiles – would provide Russia with a relatively safe zone in the High North from which it could target large parts of Western Europe and threaten maritime traffic in the Atlantic.

We know that the outbreak of the Korean War in 1950 had important implications for European security and NATO. And today we cannot rule out NATO involvement should a conflict erupt in East Asia, for example, on the Korean Peninsula, in the East China Sea, in the Taiwan Strait, or in the South China Sea. Based on the assumption that North Korea can target the continental United States with intercontinental ballistic missiles, the Trump administration contends that North Korea poses the greatest immediate threat to the US. While a North Korean missile strike against the US remains unlikely, such an attack would most likely trigger NATO's Article 5.

Russia might use a military conflict in East Asia as a pretext to intervene in NATO countries in the Baltics or Eastern and Southern Europe. Conflict between Russia and NATO could then spill over into the High North. Such a scenario would force the US to balance and prioritise between conflicts in two theatres and potentially prevent the US from enhancing its military presence in a third area, the High North. It remains to be seen whether US–China rivalry in East Asia or the North Korean crisis will trigger any conflict, and whether Russia will take advantage of any potential conflict in East Asia to advance its interests in Europe. Nevertheless, developments in East Asia are likely to shape the US' and NATO's defence planning and responses to any future conflicts.

Managing and strengthening US alliances, while competing for the alignment of smaller states, are challenges the US faces in its two flanking regions. How the US manages its alliances, and how it supports its allies in East Asia, have important implications for the credibility of the US global alliance system. If the US will not stand up for South Korea when threatened by North Korea, or if the US does not support Japan, Australia, and the Philippines, then such a stance is likely to undermine belief in a collective defence and US security guarantee – even in Europe. Conversely, if the US launches a preventive strike against North Korea without the consent of South Korea, then such unilateral use of force would have major implications for US global alliances.

NATO has become more preoccupied with deterrence and collective defence. Such challenges are also a core concern for the states of East Asia, whether in relation to deterring China's assertiveness or the more pressing challenges posed by the North Korean nuclear and missile programme. Lessons learned from deterrence in East Asia might be useful for studying how deterrence can work in Europe. Since the US is the key security guarantor in both regions, the implementation of US coercive measures that seek to deter adversaries in East Asia will probably shape how deterrence measures are implemented and sustained in Europe.

Changes in interpreting the law of the sea in East Asian waters, brought about by the rise of China and its increased capabilities, challenge the status quo and have potential implications for Norwegian maritime interests. How the US responds to China's anti-access and area denial capabilities in East Asian waters is also important for understanding how the US might address a similar challenge from Russia in the North Atlantic. US military concept, such as the Third Offset, AirSea Battle, and the Multi-Domain Battle, informs US thinking about the functions and usage of military force. The US Joint Doctrine, signed and approved in October 2016 and termed Joint Concept for Access and Maneuver in the Global Commons (JAM-GC), will not only guide US

operations in its rivalry with its peer competitor, China, in East Asia, but also describes how US forces will operate in Europe. Such concepts and doctrines seek to support and inform US and allied forces in countering rising threats to US access and manoeuvres, in sustaining conventional deterrence, and in maintaining US technological superiority in both of its flanking regions.

The development of military capabilities, new technologies, and platforms in one region does not take place in isolation. Advances in missile technology, the development of missile defence and radar systems, and enhanced space and cyber capabilities all demonstrate that the effects of military modernisation are global. How such capabilities are developed, implemented, and used in one region can affect another region. US ambitions for a global missile defence system involve cooperation with allies in both Europe and East Asia. The price, upgrading, and maintenance of the new F 35A fighter, and how these aircrafts are deployed in military operations in the years to come will be shaped by the experiences gained by the US and its allies in Europe and East Asia. The new superpower rivalry will drive developments in new technologies ranging from artificial intelligence, quantum computing, big data, biotech, nanotech, unmanned capabilities, robotics, 3D printing, and e-commerce.

States in both Europe and East Asia are adjusting to great power politics and increased rivalry. In the previous phase of superpower confrontation during the Cold War, Norway struck a balance between deterring and reassuring its adversary the Soviet Union through integration and screening within the NATO alliance. Similar patterns of behaviour are recognisable in Europe and East Asia today. The terms 'deterrence' and 'reassurance' are very much at the core of the renewed debate, as NATO seeks to find the appropriate response to Russian aggression. Norway is just one of many NATO countries that seeks to balance its ties to the alliance with continued cooperation with Russia.

These predicaments mirror those facing South Korea and Australia as they seek to strengthen their alliance with the US, while simultaneously screening in order not to provoke China. Although South Korea and Australia seek more cooperation with China, they are also developing closer ties with the US to prevent becoming too dependent on, and to deter China. Similar to contemporary developments in the relationship between NATO and Russia in Europe, East Asian states and the US are attentive to the balance between deterrence and reassurance in their relationship with China.

Similar factors are driving the strategic adjustments and policy preferences of states in East Asia and Europe. Geography, history, military capabilities, domestic politics, and economics explain not only the different balance between deterrence and reassurance developed in states such as Norway,

Poland, Germany, and Turkey as they seek to strike a balance in their relationship with Russia, but also why Japan, South Korea, the Philippines, and Australia pursue different balances between deterrence and reassurance in their policies towards China.

The future of the US' grand strategy, the credibility of its alliances, the role of deterrence, secondary states' adjustments to great power rivalry, military modernisation, and the emergence of a new world order are issues shaping current strategic thinking in Europe and East Asia. In order to gain a better understanding of these core themes, we need to examine how they overlap in the US' two flanking regions, and understand the effects of a new bipolar international system.

Perspectives on Hybrid Warfare

by Pasi Eronen

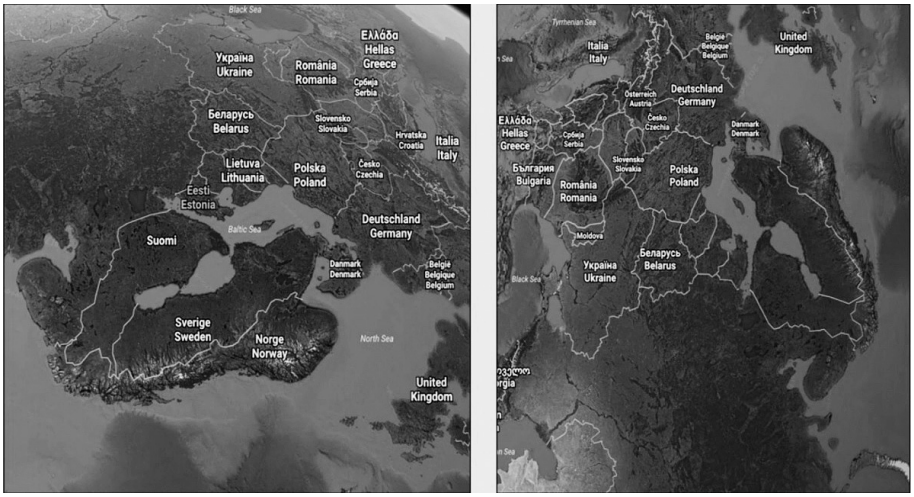


Figure 1: Inverted maps of Europe, emphasising Russia's perspective on the Norwegian Sea, Scandinavia, the Baltics, and the rest of Europe.
Source: Pasi Eronen, Center on Sanctions and Illicit Finance, Foundation for Defense of Democracy

Sometime ago, I was advised by a colleague to always bring maps when holding presentations to military personnel. Maps help to underline the importance of geography, and as you can see, the world looks different when it is oriented in different ways. This holds true both when oriented from the Norwegian Sea towards Russia, and when oriented from Russia towards Europe. Those familiar with military operational planning will be aware of how the act of turning a map around will help in setting yourself in the shoes of the actor at the other end – in this case, the Kremlin. How do the people in the Kremlin view the map, and what do they see in front of them? In the view taken from the Norwegian Sea perspective, it looks like we are fractured by the Baltic Sea, separated by geography. However, we are brought together by the region's ideologies and ideals. Furthermore, everything that happens within the triangular area ranging from the North Sea, the Arctic, and the Black Sea, bears a great significance to us all. Ukraine is a telling example of how this region matters, namely because of the local, regional power – Russia.

A changing world order?

Current economic trends in Russia are worrisome. At the same time as the price of crude oil is growing, the Russian production of oil increases. Partly because of the sanctions imposed upon Russia and the trends forced by the previous low oil prices, production costs have gone down. An example of this phenomenon is how Norway's oil industry is experiencing larger profitability these days compared to previous years when the oil price was much higher, because of how the low oil prices forced the industry to increase its efficiency. We can imagine that something comparable has happened in Russia, which means that we don't need to see prices of $150 per barrel for them to receive the same amount of resources that they received prior to 2014. This is an important realisation if we think Russia harbours malicious intent. An increase in resources will support their development of capabilities, also impacting the development of their hybrid capabilities. I also worry about whether the United States is willing to lead the current world order. Can Europe continue to trust the U.S.' willingness to lead from the front? Has the authority of the United States eroded? In a presentation I held in 2016, I emphasised that Putin's apparent strategy is to turn the post-cold war order, and increase Moscow's standing as the main geopolitical alternative to the U.S-led West, in addition to undermining the authority of the United States. Barely a year after the election of President Donald Trump, I have begun to wonder if I would use the phrases '*U.S-led West*' and '*Authority of the United States*' today.The converging and, somewhat, paradoxical trends of the erosion of U.S. authority and the growing funds of the Kremlin may influence the Russian decision-makers in such a way that they are more likely to identify and utilise windows of opportunity. This touches upon the question of a changing world order, emboldened by an increase in resources and the erosion of U.S. authority: will the Kremlin begin to believe that now is the time to act?

Hybrid warfare

This conference is about Multi-Domain Battle, so why is my remark about hybrid warfare? As the name Multi-Domain Battle implies, one could easily think that it entails the use of kinetic force. The use of hybrid tools, however, takes place in a shaping phase before the utilisation of kinetic force. This is especially important when looking at the relative strength of militaries across the world through the perspectives of budgets – you would be

right in thinking that Russia's budget looks rather small compared to Germany's budget potential if they were to use 2 percent of its GDP. Then again, it's more about where Russia is putting its money. Do they have a wider array of tools in their possession, that they are willing to utilise to attain their goals? In my opinion, a nation state has a wide array of instruments of power, which it can use to achieve its aims at the world order-level. We know that the Kremlin harbours such aims. However, whether they can attain them is a different question.To some, this may seem similar to the kind of political warfare akin to the 'Long Telegram' and 'NSC-68' from the Cold War-era. So, what is the difference? The digitalisation of a whole society, the increased speed of information, social media, the use of big data and the profiling of individuals, and the hacking of sensitive information are all elements that can be used in active measures campaigns, also called 'influence campaigns'. What we have seen across Europe is the malicious use of technology in information campaigns. One could say that this is reminiscent of the typical, Soviet-style active measures campaign, which is true, but the West has become much more vulnerable. The fully digitalised West can now be attacked from several new attack vectors, such as our privately-owned critical infrastructure. The tools available in the hybrid toolkit range from soft power to hard power tools, which include a spectrum of diplomacy, sanctions, and at the far end, the use of military force. This is where we touch upon Multi-Domain Battle. This means that we have to be able to invoke all the resources of our societies to defend ourselves, which is especially true for small powers such as Norway and Finland. In Finland, we call this 'Comprehensive security'. How can we be more proactive instead of reacting to the threats that we are facing, such as the influence campaigns on social media that we have seen in relation to various referendums and elections? After all, the campaigns were planned much beforehand, with anticipated impacts. Now they are reaping the benefits. Therefore, we should try to figure out what they will be up to next, and what kinds of tools they are planning to utilise. This touches upon the importance of international cooperation. For example, small countries cannot, by themselves, reveal the modus operandi and the patterns that are emerging from those Russian activities. We have to cooperate, share information, and be able to understand the bigger picture.

Many analysts are suggesting that the price per barrel of oil will climb back to the $100-dollar range, in addition to increased prices in natural gas in Russia's case. After Putin's solidification of power in the recent election and a better economy, some people are arguing that Russia is going to continue its mili-

tary modernisation programmes, decreasing hybrid warfare activities. I would argue, however, that we will see quite the opposite – the military modernisation and the existence of a core of hard power will back up the softer means of hybrid warfare. Therefore, we will see an emboldened and resurgent Russia, seeing their opportunities abound. Their tacticians, as we have often witnessed, will try to grasp these opportunities. With the increased flow of money to the Russian treasury, I argue that we will see a more confident Russia. Furthermore, more money and a replenishment of its reserve fund will allow Russia to buy support from its population.

Beyond Russia

In this part of the world, close to the Arctic Circle, we are, of course, seeing Russia as the mortal threat. At the same time, it is of key importance to see beyond Russia, namely China and its activities. For example, during the past summer, we witnessed the Russian and Chinese navies together in the Baltic Sea, and we are seeing Chinese trains arriving in Finland and Britain, at the far end of their 'Silk Road' project. Many of these things can be tied to China's economic development, but at the same time, it's also the development of their power and grasp in Europe. Often with these authoritarian states, namely Russia and China, we aren't talking about soft power in the way we apply the term to liberal democracies, which is more like inviting countries to take on our set of values and ways of living. We are rather talking about 'Sharp Power'; it is the utilisation of something resembling the soft power of liberal democracies but having authoritarian undertones.

Conclusion

I do realise that this seems very bleak – doom and gloom and alarmist talk, but I would like to end my remark on a positive note. Even in the presentation I held in 2016, which I referenced above, I suggested that we really need to start doing something. Reporting on events that are already ongoing means that it's already too late. We need to be more proactive. Now, however, we are starting to see positive developments, such as new legislation enabling renewed mandates to intelligence services and armed forces, and vulnerability surveys aiming to map the vulnerabilities of our governing system, surveys of which we are acting upon. We are also seeing the emergence of international cooperative structures. One example is 'The European Centre of Excellence for Countering Hybrid Threats' (Hybrid CoE) established in

Helsinki, offering a shared space of cooperation for NATO and the EU. At the same time, we need to ask ourselves if we are acting quickly enough in order to respond to the challenges following the worrisome trends related to the changing world order and shifting economic powers. As well as Russia, although a bit further away in the near future, China is definitely coming.

Stormakters vekst og fall

av Geir Lundestad

Som historiker pleier jeg å innlede med at det mange tror, særlig politikere, ikke er sant. De tror at historien gjentar seg, men dette er helt feil. Man kan ikke løfte frem den parallellen som man alltid har trodd har eksistert, som et bevis for at historien gjentar seg. Sånn er det ikke. Det som gjentar seg, er historikere, men det er noe helt annet.

I 1945 var det én makt som var ufattelig mye sterkere enn alle andre makter. Da hadde vi den unike situasjonen i verden at USA produserte like mye som resten av verden til sammen. Det har aldri skjedd tidligere i historien, og kommer aldri til å skje igjen. USAs posisjon var basert på den enorme veksten landet hadde hatt under andre verdenskrig, og de ødeleggelsene som hadde funnet sted ellers i verden. USA utgjorde altså 50 prosent av verdens BNP. Den andelen var nødt til å falle raskt – allerede i 1950 var den redusert til 40 prosent, i 1960 ned til 30 prosent og i 1975 ned til 23 prosent. En slik nedadgående kurve kan få en til å stille spørsmålet om hva som kan komme til å skje i fremtiden, og generaltabben som ofte gjøres, er at man tolker trenden som har vært, til å fortsette. I så fall vil jo USA til slutt forsvinne.

Men det som faktisk skjedde, var at kurven ble liggende rundt 21–23 prosent. Det amerikanske overherredømmet har hvilt til dels på de amerikanske militærressursene som blomstret opp under andre verdenskrig, men også på den amerikanske økonomien og på det vi kaller «soft power» – amerikansk kultur. Dette var helt unikt. Disse forestillingene spiller alltid en rolle. Fra 1970-tallet og utover hadde mange en forestilling om at siden denne kurven hadde gått såpass mye ned, ville USA komme til å bli utfordret.

USAs stormaktsutfordrere

Russland

Den første store utfordringen var selvfølgelig Sovjetunionen. På slutten av 1950-tallet holdt Nikita Khrusjtsjov en rekke taler hvor han spådde at Sovjetunionen ville komme til å vokse forbi USA på en rekke områder. Og det var ikke bare han som trodde det, men mange andre også. Selv glupe folk i Norge trodde at denne analysen var rett, og to av de aller glupeste var justisminis-

ter O.C. Gundersen og ekspedisjonssjef ved Statsministerens kontor Andreas Andersen. Sistnevnte leste Le Monde hver dag, og gikk derfor for å være litt av en storkapasitet når det gjaldt utenrikspolitisk analyse. De sa noe av det dummeste som har blitt sagt noen gang – midt på 1950-tallet – at nå som det går såpass fremover med Sovjetunionen, er Norge nødt til å gjøre noe for å få større fart på økonomien i Nord-Norge. Hvis ikke ønsker alle nordlendingene å flytte til Kolahalvøya. Selv om det ikke var slik det gikk, er det interessante med slike uttalelser at de trodde på det. Det var altså en ganske utbredt forestilling. Selv haugevis av lærde amerikanere, med John Kenneth Galbraith i spissen, trodde på konvergensteori. Teorien var et mildt uttrykk for det samme – at man må prøve å kombinere det beste fra den kommunistiske økonomien og det beste fra den kapitalistiske økonomien. Dermed skulle man få den aller beste samfunnsformen. Men vi vet hvordan det gikk. Gjennom Sovjetunionens raske opprustning og SALT-avtalen ble Sovjetunionen nesten militært likestilt med USA. Men for å være en ordentlig stormakt er man nødt til å ha en balansert tilnærming. Den store feilen som ble begått, og som særlig gjøres av de militære, er at man bare ser på de militære kapasitetene. Det er klart at det hadde funnet sted en enorm vekst i Sovjetunionen, og de hadde fått en betydelig evne til maktprojisering. Men de hadde ikke de økonomiske ressursene som skulle til.

Da Mikhail Gorbatsjov kom til makten i 1985, forsøkte han å finne ut av hvor stor andel av BNP som gikk med til de militære styrkene. Dette svaret var helt umulig å få, og han fikk det aldri. Likevel skjønte han at det var altfor mye. Senere beregninger har vist at Sovjetunionen brukte 25–30 prosent av BNP på militæret. Når USA fikk like store styrker ved bruk av bare 5–6 prosent av BNP, forsto man at dette var en vanskelig situasjon. I det lange løp var det denne forskjellen som førte til Sovjetunionens fall. Det lot seg ikke gjøre å konkurrere mot USA når man hadde en økonomi som var så mye mindre. I Sovjetunionen var koblingen mellom sivile og militære sektorer nærmest ikke-eksisterende, mens det var nettopp dette amerikanerne var så dyktige på. De klarte å bruke satsingene på romfart og militæret i den sivile økonomien. Og alle som reiste til Sovjetunionen på 1970- og 80-tallet, spurte seg selv hvordan det skulle gå dersom de ikke klarte å mestre vannklosetter. Vi vet hvordan det gikk.

Det moderne Russland står sterkt militært, men har de samme svakhetene og skjevhetene i sin totale tilnærming. Det er klart at de kan ta Krim-halvøya og lage mye ugagn i Øst-Ukraina, men de får fortsatt ikke økonomien til å fungere. Dette kommer til å bli et stort problem. Ved å stort sett eksportere olje, gass og våpen, riktignok viktige ressurser, vil et land kun klare å bygge en begrenset fremtid. I tillegg har Russland vært et land i krise. For eksempel er situasjonen rundt levealderen til russiske menn helt ufattelig. Da Gorbat-

sjov gjennomførte sine reformer på 1980-tallet, lå russiske menns levealder på rundt 73–74 år, tilnærmet likt et lavt vesteuropeisk nivå. Da reformene hadde blitt gjennomført, var levealderen for menn sunket til 58 år. Dette var en total kollaps, og vi kan vanskelig forestille oss realitetene som er knyttet til denne kollapsen. Det er verre enn om det hadde vært krig. Nå øker riktignok levealderen igjen og har for menn passert 63–64 år og er på vei videre oppover. Men de har fremdeles langt igjen. Ja, Russland må håndteres militært, men denne sosiale realiteten vitner om at det ikke er Russland som er den store utfordringen på lang sikt.

Japan

Utover 1970- og 80-tallet kom det en stor bølge av bøker som alle spådde at fremtiden tilhører den nye supermakten – Japan. Paul Kennedy, som jo har skrevet mest om stormakters vekst og fall, utga i 1987 boken *The Rise and Fall of the Great Powers*, som ble solgt i tre millioner eksemplarer. I bokens berømte kapittel åtte spådde han, riktignok i meget forsiktige ordelag, at USA var på vei ned. Kennedy, som var fra Newcastle i Storbritannia, hadde selv sett både sin bys og sitt lands vekst og fall. Og selv om det ikke alltid er synlig, finnes det jo en masochistisk streak i mange amerikanere. Som engelskmann fant han derfor en viss glede i å påstå at det kom til å gå nedenom og hjem med USA. Men så begynte Kennedy på en ny bok – *Preparing for the Twenty-first Century*. Denne ble skrevet på Det Norske Nobelinstitutt, og på tross av mine gjentatte innskytelser om at det var helt feil, hevdet han i svært kraftige ordelag at det 21. århundre virkelig tilhørte Japan. Dette baserte han på åtte variabler som han hadde fått hjelp til å tolke av et stort batteri med doktorgradsstudenter.

Problemet var at disse åtte variablene kun dekket et lite bilde; for eksempel hadde ikke demografi blitt tatt hensyn til. Allerede da boken kom ut, hadde Japan gått inn i en betydelig økonomisk og politisk krise, som de har slitt veldig med å komme ut av. Selv i dag har ikke landet kommet ut av krisen, og for tiden er det ikke en eneste forfatter som hevder at det 21. århundre tilhører Japan. Det finnes det ikke grunnlag for, selv om man ikke skal undervurdere landet. Japan er fremdeles en betydelig aktør, og det er klart at så lenge USA har Japan på sin side, samt en god del andre land, vil det begrense Kinas rolle.

Den europeiske union

Deretter kom det en ny bølge som hevdet at EU var det lovede land, som selvfølgelig var helt feil. Rundt år 2000 kom en flom av bøker om EU, noen av amerikanere som straks kom til å bekjenne sine synder. Men mange i Europa likte tanken om at EU kom til å utfordre USA. EU har tross alt langt høyere

folketall og en samlet sett større produksjon, og de hadde proklamert en felles utenriks- og sikkerhetspolitikk. Det var derimot det eneste de hadde gjort – de hadde ikke en felles politikk, de hadde kun proklamert den. En felles utenriks- og sikkerhetspolitikk er i praksis helt fraværende, og de har store problemer med å bli enige om noe som helst. Så har det vært snakket om felles militære ressurser, men det hjelper ikke at Storbritannia nå har meldt seg ut av EU. Det ble ganske fort slutt på strømmen av bøker som hevdet at det 21. århundre tilhørte EU. I det store bildet vil ikke EU bli den overordnede sikkerhetspolitiske aktøren, og dette har vi forstått i Norge, ettersom vi baserer nesten alle planer på USA.

Kina

Nå har vi i noen år vært inne i den kinesiske bølgen, som jeg trodde delvis var over. Mange har kommet frem til at det er store svakheter i Kinas posisjon, som hindrer dem i å utfordre USA i å innta den overordnede rollen. Kina har derimot fått ufattelig god hjelp av Donald Trump. Ved å basere utenrikspolitikken på «Make America Great Again», hvor alt dreier seg om USA, gjør han sitt beste for å skade landet sitt. USA har tross alt vært det ledende internasjonale landet fordi de har representert brede, internasjonale interesser. Det var derfor vi likte Woodrow Wilson, Franklin Roosevelt og de mer moderne variantene. Her kommer derimot President Trump og sier at han bare bryr seg om USA. Riktignok føyde han til i Davos-talen i 2018 at USA ikke er alene, men det var ikke ett eneste ord om de globale utfordringene. Hvis man leser amerikanske myndigheters strategidokumenter, ser man at Trump ikke har fått gjennomslag i sin egen administrasjon. Utfordringene som skinner igjennom i disse dokumentene, er Russland og Kina. Trump, derimot, har ikke sagt et eneste negativt ord om Russland, og kongressen har vedtatt lover som forhindrer han i å følge opp overfor Russland. Vi får se hvordan det går med Trump, etter at alle disse forbindelsene han har til Russland, kommer frem gjennom Muellerkommisjonen og dens granskingsprosess.

Men tilbake til Kina. Det er flere argumenter mot tidligere analyser om Kinas fremvekst. For det første er flere av dem så optimistiske på Kinas vegne at det heller ikke er Kinas egen analyse. Dersom man studerer hva det kinesiske lederskapet har sagt, er de beskjedne i språkbruken. I en debatt for bare noen år siden snakket kineserne om «Peaceful Rise». Dette fant de ut at var litt for utfordrende, og de kom frem til at man heller kanskje skulle snakke om «Peaceful Development». De har heller ikke på noen som helst måte glemt Deng Xiaopings advarsel om å snakke lavt om Kinas vekst. Og når Xi Jinping snakker om det fremtidige perspektivet, er tanken på å utfordre USA i å ta over den

dominerende rollen helt fraværende. Han snakker om 2049, når det er 100 år siden revolusjonen. Da begynner vi å snakke om et langsiktig perspektiv, men, som vi vet, kan vi ikke skrive om alle trender fremover i tid. Kina begynner også å få problemer med veksten. En tidligere kinesisk statsminister ble spurt om hva som bekymret han, og det var hvis Kinas vekst falt under seks prosent. For øyeblikket ligger den på litt over seks prosent, men den kommer til å falle under. Da er det viktig å huske på at avtalen som det kinesiske folket har med lederne, handler om seks prosents vekst, og folket holder munn. Hva som da skjer når veksten går under seks prosent, er ukjent.

Det som er USAs aller største fortrinn, men som Donald Trump gjør sitt beste for å underminere, er landets mange alliansepartnere rundt om i hele verden. Kina har et helt annet utgangspunkt. Kina ønsker ikke allianser, og de alliansepartnerne de har, er av meget tvilsom verdi – de landene som står nærmest Kina, er land som Nord-Korea og Pakistan. Da er det forståelig at Kina ikke er så interessert i allianser. I en artikkel skrevet av Michael Beckley for tidsskriftet *International Security* går han i detalj gjennom den militære situasjonen i Sørkinahavet. Der viser han at den kinesiske situasjonen heller ikke militært er spesielt god. De aller fleste landene i regionen, slik som Vietnam, Indonesia, Japan og India, har også rustet opp betydelig. Til sammen har de rustet opp nesten like mye som Kina. En viktig faktor er også at i tilfelle militær strid skulle forekomme i Sørkinahavet, befinner en rekke av disse statene seg i geografisk nærhet til begivenhetens sentrum. Kina har en langt lengre forsyningslinje.

I tillegg er det mange andre problemer. For eksempel er Kina helt gale etter å få nobelpriser, og kinesisk-amerikanske nobelprisvinnere blir feiret når de kommer til Beijing. Myndighetene forsøker systematisk å kjøpe dem opp og gi dem alt mulig av ressurser. Likevel er det svært få som reiser tilbake til Kina. Landet har en ambisjon om å vinne nobelpriser, men de som landet vinner, er fredspriser og litteraturpriser som de helst ikke vil ha. Videre har det nylig vært en hærskare av skandaler i kinesisk forskning. Mens vi i mellomtiden har vært svært fascinert av talene som omtaler antallet doktorgradsstudenter og universitetsansatte, patentsøknader og lignende, har de ikke fått noen nobelpriser innenfor vitenskapen. Det har kommet frem en rekke påstander om plagiat og andre alvorlige forhold. Kina har et stort problem hva gjelder det som er helt avgjørende for all moderne vitenskap – originalitet. Østasiater, inkludert japanere, har en veldig respekt for forfedre. Det kan høres flott ut, men det er et helt elendig utgangspunkt for moderne forskning, hvor man skal forkaste omtrent alt de eldre har stått for.

Glem ikke USA

Jeg tror egentlig ikke at historien gjentar seg, men konklusjonen min er at vi ikke må glemme USA. Donald Trump varer ikke evig, selv om han kanskje sitter ut perioden. Men selv med Donald Trump er USA en sentral aktør, ikke minst her på Værnes, hvor de plutselig har blitt en lokal aktør. Det har de aldri vært før. Videre ser vi at USA har nesten 100 000 soldater i Europa, inkludert i land hvor de aldri har hatt det før. Igjen: Dette er ikke noe Trump ønsker. Likevel går verden sin gang, til tross for alt Trump har sagt. Alle de øverste amerikanske sjefene vet godt hvordan situasjonen er, og forsvarer politikken med at USA er nært knyttet til et NATO som Trump har kalt avleggs. Tvert imot ser det heller ut som at amerikansk tilstedeværelse bygges ut. Likevel må vi minne amerikanerne på at deres ledende posisjon ikke varer evig uansett hva som skjer – etter amerikanernes egen tro vil posisjonen bestå fordi den er bestemt av Gud. USA har mange betydelige utfordringer. Men det har vist seg at alle som har utfordret USA, med et delvis unntak for Kina, ikke har ført til at verden har blitt bipolar. Det er helt absurd å hevde at verden er bipolar nå – men man kan derimot se for seg at det kommer til å skje tjue–tretti år frem i tid, dersom man fremskriver alle tendensene. Det bør vi ikke gjøre.

Joint Concept for Access and Maneuver in the Global Commons (JAM-GC)

by David W. Hicks

The Joint Concept for Access and Manoeuvre in the Global Commons (JAM-GC) is of a classified nature, and the concept is also evolving. We are using it as a concept in the Joint Force in the United States in order to solve a problem that we didn't necessarily create, but which has evolved over time. This happened because we, to some degree, ignored world events, and took our eyes of the ball regarding what our adversaries have been doing for the last 20-25 years.

Combined, the U.S. and our allies are a global power with global interests. With those global interests, we need to abide by the rules of international law, and free and open trade. In addition, we need free and open access to the global commons around the world, such as sea lanes, airspace, space itself, and cyberspace. Since the end of the Cold War, we have had no real challenges to that access. There has been no adversary that has tried to keep the U.S. or our allies from penetrating anything that we consider global commons in any of the previously mentioned domains. That ease of access has allowed our thinking to evolve away from worrying about it. However, over the last 10-15 years, the rise of Anti-Access/Area Denial (A2/AD) challenges and threats by certain adversaries has allowed them to become a threat to us and our freedom of access to the global commons. The importance of this access is best underlined by General Joseph F. Dunford, Chairman of the Joint Chiefs of Staff: '*At the operational level, our ability to globally project power is a key military centre of gravity*'. Our ability to project power anywhere around the globe, in any domain and at any time, has been what has allowed the U.S. and our allies to have freedom of manoeuvre for the last 50-60 years. U.S. security commitments and guarantees are at risk, putting the credibility of our alliances and treaties on the line, and, obviously, the ability to manoeuvre inside the global commons.

The challenge

How do we maintain the freedom of action in spite of these advanced threats designed to prevent access and disrupt manoeuvre? As of late, we have seen a rapid advance in and proliferation of A2/AD technology, which has happened in a changing world in terms of threat characteristics. At the same time as we are seeing the rise of traditional threats such as Russia and their re-emerging capabilities in both nuclear and conventional force, we are seeing the rise of China as an actor on the global stage, which has also developed similar capabilities over the last 10-15 years. Furthermore, we have regional threats such as Iran and North Korea, the latter of which can also represent a global threat. The range, lethality, and sophistication of many of our adversaries' weapons continue to grow, to the point that they are currently outpacing some of our capabilities. In addition, the threat is occurring, growing, and evolving across all domains.

One way to think about this is how we, 20-25 years ago, limited our thoughts to the air, sea, and land domains when we talked about military operations. The cyber-domain has not, as of yet, even been defined. Now, however, cyberspace is an area where we are being contested every day. The same can be said about space – 25 years ago, we thought about space as a place where we had satellites which ensured communication, weather reports, and GPS. Now, space is currently being contested, and starting to be disputed by some of our adversaries' capabilities, and what they potentially can do to us should they want to.

The contested environment

What does this environment create? First of all, communications are disrupted, hindering our ability to do Command & Control (C2). It also creates threats to the space systems, such as surveillance, reconnaissance, communications, and navigation. It creates cyber-attacks against networks, communications, and weapons systems. Furthermore, the environment has created our adversaries' ability to employ ballistic and cruise missiles attacks, both against land targets and anti-ship. (In the U.S. Airforce's context especially, the fact that we have not been contested in such a way is what has allowed us to operate from large bases around the world). We are seeing electronic and directed energy capabilities such as the lasers that our adversaries are developing, and mine warfare. Also, C2 and sustainment are under stress because of their reliance on space, cyber, and those assets' roles across all the other three domains, which are crucial for having all domains working together. If any one of these is taken out, especially space or cyber, our ability to fulfil

operations anywhere around the world, day in and day out, would be greatly hindered.

This is the contested environment that we are dealing with, and JAM-GC is about trying to get us to think differently about how we want to operate in this environment.

What is JAM-GC?

JAM-GC originated in 2009 when the Navy and Air Force were tasked with collaborating to develop a comprehensive Air-Sea Battle Concept and associated initiatives to counter emerging A2/AD challenges, such as in the South-China Sea and the first Chinese island chains. Thus, the driver behind the concept has been how to do just that. It is of a similar mindset to how we created the Air Land-Battle concept for the army decades ago. Eventually, they realised that the developing concept should not be limited just to the Navy and Air Force. In 2015, the Director of the Joint Staff ordered the ASB concept to be revised. By 2016, the concept was renamed JAM-GC, which were to build on ASB's best ideas and lessons learned so far. In July 2017, the JAM-GC's transition plan was put into place.

Central themes

JAM-GC describes how Joint Forces will maintain freedom of action in an environment where adversaries employ advanced capabilities to deny access and disrupt manoeuvre in the global commons. The central idea is to create a distributable, resilient, and tailorable force, employed in sufficient scale, and for ample duration, to maintain access and manoeuvre in and through the global commons. Lines of Effort (LOE) are 1) Set Conditions before Crisis, 2) Fight for Decision Advantage, 3) Defend in Depth, 4) Attack in Multiple Domains, 5) Sustain the Distributed Force.

JAM-GC is not rocket science and is not about inventing earth-shattering new technologies. It is all about putting hard thought into how to make the Joint Force fight and synchronise better in both the traditional and new domains, and how to do that against an adversary that will be contesting us in those domains.

Building blocks: The five primary tenants of JAM-GC

The first primary tenant is '*Distributable*', which is the thought that our forces should be able to disperse, reposition, and use a variety of operation locations, while retaining the ability to manoeuvre and concentrate combat power.

The second is '*Resilient*', which entails the ability to recover rapidly from adversity and setbacks, which often come in the form of combat losses. For the last 20-25 years, we have fought adversaries in mostly low-risk environments, such as Iraq and Afghanistan. In an A2/AD-environment, however, we have to assume that we will be operating with a much higher risk and can probably expect to take losses that in the last couple of decades would be deemed unacceptable. Because of the enemy's capabilities, it will be getting a much greater vote. This means that we have to be resilient – that we are able to take a hit while retaining our ability to hit back.

Third is *'Tailorable'*. These days, forces need to be commanded, controlled, and employed in a temporary or permanent structure to accomplish assigned missions. That means that we have to be able to tailor our forces in a way which meets an adversary's capabilities, in order to either deter or counter them in a fight. This thinking does not limit itself to the traditional domains, being land, air, and sea; it also applies to how we must be able to contest the cyber and space domains, across all of them.

The fourth primary tenant is '*Sufficient Scale*', which is about having increased capacity to include range, carriage, and loiter times of existing platforms, including in partnered operations. It is also about the increased use and integration of commercial systems. Furthermore, it relates to us continuing the development of technologies we need to counter the adversaries' increased capabilities across the domains. Examples are using and improving advanced weaponry, such as the F-35, to counter our adversaries' capabilities in space and the cyber domain. In short, it is about expanding the competitive space in a fight against potential adversaries. Crucially, this must be done without losing connectivity between our capabilities in all domains, maintaining our ability to command and control them.

Fifth is '*Ample Duration*', which can also be called staying power. One of the most overlooked aspects in scenarios against an adversary that has near or better capabilities than we do, both in potential combat and in operating across the global commons, is logistics. This means that we have to ensure the ability to maintain the logistic needed in order for us to continue a fight for longer than what we are expecting. Over the last 20-25 years, the logistics train of U.S. deployments in conflicts has largely been uncontested, and we haven't had to worry about an interruption in any of our logistics. That will certainly not be the case in an A2/AD environment where an adversary is fighting back aggressively.

JAM-GC vs. ASB – *Similarities*

There are several similarities between JAM-GC and ASB. Both concepts realise that Joint Force must achieve and maintain freedom of action before it can project power and execute operations, and that the problem set is contested environments created by A2/AD. They also share a mutual goal, which is freedom of action in the global commons. They have similar elements, such as emphasis on integration, countering A2/AD threats, on C2 and allies and partners. They also share emphasis on being multi-domain, multi-service, multi-functional, and multi-national.

JAM-GC boils down to how we have to be good not only at fighting Joint, but also with allies and partners, against a near-peer adversary. That means that we have to be connected and networked in everything we do, in addition to our assets being compatible, enabling them to be commanded and controlled across the domains. Although this doesn't mean that we have to have the exact same aeroplanes, tanks, or radios, we do have to train with what we have, making sure that our differing equipment is compatible with both nations' and other services' equipment. Lord knows that we, in the U.S. military, have our share of scar tissue with trying to be compatible even with our own services. Our need for compatibility across services overlaid with how critical the multi-national aspect is going forward, in a time with additional domains, is the root problem which JAM-GC is trying to solve.

JAM-GC vs ASB – *Differences*

JAM-GC is about all forces, whereas ASB is limited to the U.S. Navy and U.S. Air Force. In JAM-GC's Joint Force characteristics, there is an emphasis on distributability and resilience, and acknowledgement of numerical disadvantages. The *how* has also been changed – the ASB was oriented on an adversary's systems, focussed on 'Disrupt, destroy, defeat' to break an adversary's kill chains and modify the environment. JAM-GC, however, is oriented towards the adversary's plan, and defeats the intent of the A2/AD or the problem which the enemy is posing to us. Furthermore, it recognises the temporary nature of success – the fight will be continuous.

JAM-GC – Impact

The concept does not aim to go after one answer to solve everything. It is rather an acknowledgement of some problems which have been brewing as a result of both additional domains and what our adversaries have been doing over the last 20 years. The concept is intended to aid commanders, planners, and force developers. In addition, it helps us in how to better plan operations, employ existing Joint forces in innovative ways and with Lines of Effort.

Perhaps the most important aspect is how it will help us to develop our forces, both that of the U.S. and our allies, including how we would potentially fight together. The aim is to develop a force that, with allies and partners, can maintain access and manoeuvre in a contested environment where freedom of action in the global commons is challenged. The concept looks at the necessary activities in order to do so, particularly education and integrated training. The concept also advocates new capabilities and approaches.

JAM-GC is a foundational concept to, among other things, Multi-Domain Battle. Currently, we are hoping to get the concept 'off the ground', and continue to develop it over time.

Air Power, 'Anti-Access/Area Denial', and 'Multi-Domain Battle'

by Frank Gorenc

The Strategic Concept of NATO is collective defence, crisis management, and cooperative security. Of course, since NATO is a defensive alliance, deterrence, avoiding a conflict, has been the key goal underpinned by Article 5 of the Washington Treaty. Allies focused successfully on collective defense and deterred the Soviet Union throughout the Cold War. At the end of the Cold War as the security environment transitioned to a unipolar world, NATO Allies transitioned their focus on crisis management and committed to out of area operations in in the Balkans, then Afghanistan during the fight against terrorism. In the meantime, a more aggressive and discontent Russia reappeared under the leadership of Vladimir Putin to annex Crimea and extend their reach using a new approach called hybrid warfare. A reenergized and rearmed Russia alarmed many Allies, particularly the Baltic nations. Since Crimea, NATO has pivoted back to collective defense, Article 5 and deterrence against a near peer capable Russia.

On the other side of the planet, China is also expanding their reach with a vibrant economy and a growing population. China is on the rise and disturbing the rules based international order using methods that do not challenge the conventional strength of the Alliances and coalitions directly. Both China and Russia know that they can not win a direct conventional confrontation with NATO or a coalition of the willing so their actions are all designed to stay below the threshold of conventional conflict, create fissures among Allies and challenge the international rules that have maintained security and stability for decades.

Throughout the change in the security environment, NATO Joint Air Power (JAP) delivered five essential capabilities to the Alliance: air and space superiority, strike, Intelligence, Surveillance and Reconnaisance (ISR), mobility and the Command & Control (C2) to the Alliance. NATO JAP was flexible,

timely and effective in it's role of underpinning deterrence during the Cold War and facilitating the fight against terrorism. Today, NATO JAP continues to meet the needs of the Alliance, along with coalition land and maritime forces.

The future will be challenging against near peer adversaries, particularly Russia will be challenging. After the Cold War and throughout the fight against terrorism, NATO air forces have gotten smaller and the people, equipment and training have been overused and not modernized. The ability to conduct a high end fight against a well equipped near peer adversary in a contested environment has been degraded. On top of that, new domains such as cyber and space have emerged. Additionally, new technologies such as ballistic missiles have reduced the normally overwhelming conventional advantage of the NATO Alliance.

To meet the challenge, the sovereign nations of NATO continue to organize, train and equip their national forces. Interoperability is pursued within the Alliance with standards in procurement and training so that when a NATO force is being generated, the nations volunteer combat ready forces. After force generation, the military leadership within the NATO Command Structure (NCS) would execute the NAC mission within assigned authorities, ROEs and special instructions. Allies would also submit national caveats to further clarify their nation's instructions to their nation's deployed force.

During execution at the tactical level, the air commander would employ the generated force to execute the kill chain: Find, Fix, Track, Target, Engage and Access (F2T2EA). This 'kill chain' methodology was expertly developed during the war on terrorism. However, the ability of the NATO air component to execute this kill chain in a near peer fight in a contested environment will challenge even expertly trained Airmen flying the most capable 5th generation aircraft. Contested or denied environments could bring combat losses well above those experienced during the war on terrorism. To meet the threat in contested environments, the NATO force will have to elevate their capabilities through the synchronized and integrated effects across all of domains; air, space, cyber, land, sea and under sea. Multi-domain operations or multi-domain battle will be the key to enhancing deterrence and achieving collective defense.

Multi-Domain Battle

Emerging capabilities in space and cyber have brought new focus onto multi-domain. Multi-domain battle is not simply joint warfare. Multi-domain battle is synchronizing and integrating the capabilities of all domains in the effort to

exponentially increase the combat capability of the whole joint force. Tactically, the multi-domain opportunities to make more effective the kill chain will give commanders more options to take out targets. The effects could be lethal or non lethal, permanent or temporary, kinetic or non kinetic in all domains. This multi-domain flexibility will require the development of multi-domain C2 to most effectively use the force available to the commander.

Anti Access/Area Denial (A2/AD) – What is different?

Simply put, combat forces since the beginning of time have attempted to limit access and deny area to adversaries. Only now, it is possible for even relatively weak nations to procure readily available technologies and weapons systems that effectively create A2/AD environments in almost any domain. NATO has just come out of a conflict where the forces had complete air dominance and were unimpeded from operating anywhere on the ground. NATO's ability to achieve air dominance in the future is in question. Future combat operations will be conducted in contested or even denied environments in some or all domains. For example, today Kaliningrad is the best defended piece of airspace in the world and any combat operation in and near Kaliningrad would be difficult if not impossible. A2/AD environments are created to degrade or defeat the overwhelming conventional power possessed by NATO. A2/AD environments combined with adversaries using hybrid warfare below the threshold of Article 5 will challenge the Alliance in the future. Adversaries understand and accept the fact that the NATO Alliance in Europe and the United States and it's partners in the Pacific possess overwhelming capabilities.

Therefore, both Russia and China use their elements of national power (diplomacy, information, military and economic) in ways that leverage their national strengths and minimize their national weaknesses. They use their geography to leverage their elements of national power in ways that make potential responses impossible or slow. They operate below the threshold of conflict to avoid a direct confrontation against the Alliance or coalition of the willing. Meanwhile, the United States, Allies, and partners continue to employ national power in a linear, predictable fashion. This playbook exhausts diplomacy, economic tools and informational power first, then transitions to military power last. Adversaries know the playbook and will use this playbook against us as they use asymmetrical approaches buttressed by operations in emerging domains using emerging technologies. In the future, the western playbook may have to be changed to better deter or defeat the enemy.

The effects of A2/AD

In peacetime, A2/AD environments give adversaries an ability to coerce and intimidate Allies and partners. The Kaliningrad Integrated Air Defence Systems (IADS) reach spills over into Poland, Germany and the Baltic nations. As Russia flexes their muscle in Europe, the increasing number of A2/AD environments proliferating in Europe clearly demonstrates their willingness and openly displays their upgraded equipment. AD/AD environments will challenge any reinforcement effort that might be called for in the event of crisis. Simply put, in peacetime AD/AD environments could delay reinforcement, limit gaining consensus in time to make a collective defense and could erode deterrence.

In wartime, A2/AD environments will consume resources and take time to defeat.. Additionally, it could affect national decision making in a very powerful way. For instance, when President Obama was briefed on potential military action in Syria, he was told that it would take 300 aircraft and an unlimited amount of time to take down the Syrian IADS, an IADS made up of 1970 era weapons systems. Compared to todays state of the art mobile systems in Kaliningrad, , the calculus on time and resources required to take out future systems will make the decision to execute a collective defense difficult indeed. An effective A2/AD environment can quickly neutralize our asymmetric advantages in air, land, and sea domain.

Accept four realities

NATO is the most successful Alliance in history but past performance does not guarantee future results. Four realities could limit NATO aspirations: 1. NATO potential power is not real power, 2. When deterrence fails, prompt consensus is pivotal, collective defence must be decisive, 3. The enemy has a vote and could choose war, 4. NATO forces must be ready, deployable and sustainable to be fully combat capable. Recognizing and understanding these four realities will posture the Alliance for future success.

The Power Reality: NATO potential power is not real power

Today, NATO economic and military power is unmatched. However, Alliance power is potential, not real power. A $36T combined GDP does not generate real military power unless Allies increase defence spending and invest wisely. Large, well-equipped militaries do not generate real military power unless forces are fully combat capable and then offered during force generation.

The Transition Reality: When deterrence fails, prompt consensus is pivotal, collective defence must be decisive

Potential adversaries know consensus is a NATO center of gravity and will attack using asymmetric means to delay or prevent consensus. Consensus pivots Alliance mindset from peacetime to crisis and from prudent thinking to detailed planning. Consensus pivots Allies from pre-deployment preparation to execution. Long, contentious delays in gaining Alliance consensus weaken NATO credibility because the enemy may come to believe NATO would not or could not invoke Article 5. To remain credible against the threats described in Warsaw, prompt consensus must be followed with decisive real power collective defence.

The Threat Reality: The enemy has a vote and could choose war

While effective for decades, NATO deterrence could fail and the enemy could choose war. Currently, in 'peacetime', Russia, ISIL/Da'esh and Iran are aggressive and undeterred. Unattributed cyber warfare continues to threaten Allies. Russian modern long-range surface-to-air missile (SAM) systems and surface-to-surface missile (SSM) systems create anti-access/area denial (A2/AD) areas to hinder NATO freedom of movement and threaten critical infrastructure. A well-executed military campaign will be required to neutralize A2/AD.

Adversaries are pursuing and threatening the use of nuclear weapons. Russia's 'Escalate to Deescalate' nuclear strategy, the implied willingness to use nuclear weapons in response to an Article 5 response could delay or prevent consensus. Success of this strategy, real or perceived, will provide incentive for future adversaries to seek nuclear weapons and explains Iranian attempts to build a nuclear arsenal.

The Force Reality: NATO forces must be ready, deployable and sustainable to be fully combat capable

NATO leaders set high expectations for the Alliance force. They want a force that can deter, reinforce and defend against full spectrum potential threats attacking from any direction! Additionally, they want the force to be a deployable, sustainable, interoperable, heavy, high-end, full range and at high readiness!

To be fully combat capable, this force must be ready, deployable, sustainable and available every single day and it will be expensive. How expensive depends on the following unanswered questions: (1) Ready for what? (2) Deploy to where? (3) Sustain for how long?

NATO Joint Air Power core roles remain indispensible to credible deter-

rence and decisive collective defence. Command of the air, precision strike, ISR, strategic mobility and C2 will continue to guarantee success and minimize risk during both peacetime and crisis. If deterrence fails and the enemy chooses war, NATO air forces with their speed, flexibility, range and high readiness will be the first to respond and maximize the effectiveness of the follow on joint force. NATO Joint Air Power effectively integrated with the selected COA provides the best opportunity to meet Alliance aspirations. Defence investment and pursuing key urgent priorities will make NATO Joint Air Power the historical advantage Allies have come to expect.

Back to Basics 101

After accepting reality, the following list proscribes several actions that could help meet NATO aspirations. They are not listed in any order but all should all be considered.

- Meet the 2014 Wales Summit Defence Pledge of 2% of GDP.
- Improve Airfields, Increase Interoperability, Procure more Weapons, invest in BMD, Persistent ISR, Air to Air Refueling.
- Improve education and training by chartering working groups on A2AD, Air Defense, Deterrence
- Encourage Wargames using senior political and military leaders
- Replace the current standing NATO mission of Air Policing with Air Defence
- Develop operational Indications &Warnings that inspire action or accept risk
- Allow military planning prior achieving consensus
- Establish a standing, fully functional Air Operations Center that operates 24/7, 365 days a year
- Establish a standing, fully functional PED & Targeting Center that will enable the rapid employment of JAP if needed

Back to Basics 201 to Restore Western Overmatch

To restore western overmatch, western Allies and partners should pursue several emerging technologies including:

- Artificial Intelligence
- Machine Learning
- Robotics
- Big Data Analysis
- Autonomous Learning Systems
- Human-Machine Collaborative Decision-making
- Assisted human operationsd
- Advanced manned-unmanned systems operations
- Networked autonomous weapons
- High Speed Projectiles

'Multi-Domain Battle' – The Concept

by Michael D. Runey

As I discussed what's new about Multi-Domain Battle with one of my mentors, he reminded me that leaders of prior generations, the Cold War-generation in particular, have much to pass on to both the currently serving senior leaders in uniform, and young cadets and officers. To understand and implement Multi-Domain Battle is a multi-generational problem, not just a multi-domain problem. Furthermore, the mentor underlined that the Greeks and the Persians were also multi-domain.

When thinking about what is different with Multi-Domain Battle, I think we would say that we can do multi-domain, and have been for a long time, but our adversaries can now do it in a different way, often with greater speed – offsetting what we can currently do. They can be more effective in certain circumstances (although not all), challenging us in ways that, frankly, we find quite difficult to defeat. This can be true both in armed conflict and hybrid warfare, the latter of which we call 'competition'.

In December 2017, the United States Army Training and Doctrine Command (TRADOC) published 'Multi-Domain Battle: Evolution of Combined Arms in the 21st century', which is Multi-Domain Battle seen from the Army's perspective. However, just as it was published, the then Head of TRADOC, General David G. Perkins, ordered us to immediately begin working with version 2.0.

In this remark, on the concept of Multi-Domain Battle, I will address the gaps that made the first version insufficient. Furthermore, I will highlight how the Army is solving and framing the problems related to Multi-Domain Battle on an operational level. To frame the remark, it is important to note that concepts are hypotheses about what we think we might want to do. Doctrines, however, are how we fight today or will be able to in the close future. With the concept we are developing, we are trying to bring how we will fight in 2035-2040 closer to the present. At the same time, the doctrines continue to move forward. In effect, we are bringing the timelines together. In terms of this concept, at this point, the United States and its allies cannot fight, but they need to be able to move quickly in that direction.

Operational Environment

Are we really being contested in all domains? If you don't think we are, you might say that there's no need to develop a new concept. Russia and China, however, have figured out ways to contest us in all domains in order to achieve their strategic objectives through relatively short campaigns in conflicts. More importantly, they can achieve their strategic aims over increasingly longer periods in the stage below armed conflict – moreover, they're able to combine the two. Their strategic and operational approaches are, as we would say, already converged. There are several implications of this new operating environment:

Contested in all domains and environments. *Adversaries:*

- Threaten U.S. advantages in the air, maritime, space, cyberspace, and land domains, as well as the electromagnetic spectrum and information environment
- Attack systems critical for integration joint operations

Increased lethality. *Adversaries:*

- Employ weapon systems with increased capability and capacity
- Challenge friendly forces' overmatch across an expanded battlefield

Complex environment. *Adversaries:*

- Operate in densely populated areas
- Accelerate adoption of new technological and information developments
- Use of regular and irregular forces with criminal and terrorist enterprises
- Modernise or obtain weapons of mass destruction/effect

Challenged Deterrence. *Adversaries:*

- Integrate all elements of national power (DIME)
- Use proxies and surrogates to avoid direct confrontation
- Neutralise Joint Force strengths from deployment through employment

Proposed Combined Framework

Our adversaries have expanded the battlefield in four ways which are linked together – geography, time, domains, and proxies. They are increasingly able to affect our homeland from theirs in ways that they never have had before. Our adversaries are developing advanced long-range missiles and hyper-glide systems, which means that they can reach us kinetically.

They can also reach us in the space and cyber domains, and through electronic warfare. Our adversaries understand that if they take a cyber action in our homelands, be it Oslo or Washington D.C., that the action, depending on the target, can have a tactical effect. For example, an information attack on the soldiers stationed at Fort Hood, including against their families, can affect how we are able to project power out of our support areas, with immediate effect because of the way we are networked. We have not dealt with this effectively. Lastly, our adversaries are using proxies. For example, the Balkans can become a proxy-area which adversaries can start to use to get to us.

Many in the United States say that we are currently at peace. However, that notion of a peace-war paradigm is no longer sufficient. Our Cold War forebears remind us that that was competition. Although we didn't call it competition, we were actively competing with the Soviet Union. Many of us currently in uniform have lost this perspective, and we need to regain it quickly, so that we can actively and effectively compete below the threshold of armed conflict. Our adversaries are certainly doing so, and we think that they are generally more effective at this than we are, most of the time, especially in their near-abroad.

Threat Military Systems in Competition

We want to win in everything, including in the areas short of armed conflict. The military has a role in this. This requires that we think holistically – from homeland to homeland, and everything in between. Whereas the AirSea Battle doctrine primarily thought about threat systems, a vital aim of MDB is to understand what Red's campaign plan is – what are they trying to do and accomplish short of armed conflict?

One thing they are attempting is to separate alliances among nations to create conditions furthering their strategic ends. This happens over a long period of time. Conventional forces, as complex as they may be, are only one element of the systems that our adversaries have been building. The Russians and Chinese use the term 'unconventional warfare' in ways that we don't, being more active and assertive with it. For example, by using conventional forces

to create a reality on the ground to support an information campaign in close areas, such as in Northern Norway, the Balkans, or Southeast Europe. These systems are not only independent, but also interrelated. Our adversaries' goal is ultimately not to go to conflict either – if they can achieve their strategic aims short of armed conflict, they will. We have to be able to defeat this.

Threat Military Systems in Armed Conflict

We also have to be ready and able to defeat what they are attempting to do in armed conflict. Enemy forces' key idea is to fragment Joint Forces simultaneously across domains and in depth to enable manoeuvre, seize limited strategic objectives, set defence, consolidate gains, and return to competition on favourable terms to the threat.

Our problem is that we have a hard time in reaching the battlefield – getting to the fight. Especially so for the U.S. Army, which demands high costs and takes a long time to respond to a situation. The U.S. Air Force is far quicker, however, but if we don't have sufficient land forces to help in a calibrated response, we are completely out of position. It is unknown how long adversaries can separate a Joint Force, but we think that they plan to be able to do it for long enough in order to achieve their operational objectives and strategic ends. They are designing their efforts for this purpose.

Simultaneously, they are separating us in ways which largely strip us of our air superiority, specifically in intelligence, surveillance, and reconnaissance (ISR). The US Army has relied on ISR through a diverse range of systems: the Air Force, as well as our own systems such as Unmanned Aerial Systems (UAS), both from in space. However, our adversaries have managed to strip us from this. Typically, our land forces operate in the blind. When Red can isolate us, it becomes a real problem. Again, our adversaries' aim is to achieve this in a limited period necessary to achieve their campaign objectives.

What do our adversaries do next? Typically, they will initiate tactical and operational defence, forcing a coalition to raise and escalate any type of response. This may create a separation within the coalition on whether or not we are willing to escalate. What price are we willing to pay, given that our adversaries have weapons of mass destruction? Thus, in some cases, the burden of escalation falls back on us, which is a poor position to be in.

Multi-Domain Battle Problems

How does the Multi-Domain Battle Concept counter these issues? We have broken it down into five problems:

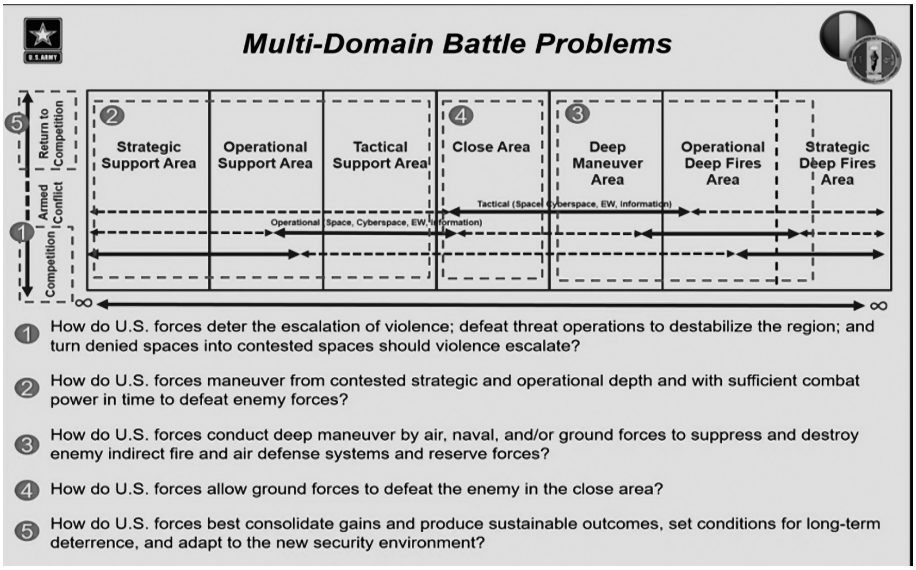


Figure 1: Multi-Domain Battle Problems in «Multi-Domain Battle»- The Concept
Source: Colonel Michael D. Runey, Air Power Conference 2018, Royal Norwegian Airforce Academy

1. How do U.S. forces deter the escalation of violence, defeat threat operations to destabilise the region, and turn denied spaces into contested spaces should violence escalate?
2. How do U.S. forces manoeuvre from contested strategic and operational depth, and with sufficient combat power in time to defeat enemy forces?
3. How do U.S. forces conduct deep manoeuvre by air, naval, and/or ground forces to suppress and destroy enemy indirect fire and air defence systems and reserve forces?
4. How do U.S. forces allow ground forces to defeat the enemy in the close area?
5. How do U.S. forces best consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?

Problem 1 is where we should and do spend most of our time. This comes down to a deterrence problem – what the enemy will attempt to do is to deny access to a space in a certain period of time. To deter this, we need to have a proven capability of immediately challenging the threat initiative. Also, we always have to be able to compete and defeat those non-lethal threat systems below the threshold of armed conflict.

Problem 2 regards how to rapidly conduct operational and strategic manoeuvres from depth, within days, not weeks or months, with a sufficient Joint Force to counter Red's campaign plan. Considering Anti-Access/Area Denial (A2/AD), this is a tough problem, especially for land forces.

Problem 3 relates to the Deep Manoeuvre Area. In the concept, this is defined as places where ground manoeuvre forces must be able to go in order to achieve Blue's campaign objectives, wherever they might be. Although we also project power through assets in the air, space, and cyber domains in these areas, we specifically need ground forces to manoeuvre into those. However, that will be difficult, due to the enemy's integrated air defence system. Their centre of gravity is their precision strike complex, both surface-to surface and air-to-surface, and is largely able to efficiently contest the area, and impose high costs to us. Clearly, the fifth generation series of aircraft we are developing, are important tools to penetrate these defences. The ability to integrate air forces through cyber/electronic means with land forces, and vice versa, is going to become an important piece to help solve the third problem.

The Army's focus is mostly on the Close Area, relating to the fourth problem; how do U.S. forces allow ground forces to defeat the enemy in the close area? This is where all good war fighters spend most of their attention. The Marine Corps is also most interested in the Close Area. This is not because they are just fixated on winning the close fight, but because they have other concepts that link the Close Area fight to problems 2 and 3. The U.S. Army haven't addressed this sufficiently.

In summary, by asking how the situation looks in time, in space, by domain, and by actor, these five problems have been hugely helpful for the U.S. Army in understanding what the enemy's threat systems are, and what they are trying to do to achieve with their campaign plans.

Multi-Domain Battle Solutions

How do we solve these problems? We argue there are three components to the solution, and I'll briefly touch upon them:

- Calibrate Force Posture
- Converge Capabilities
- Employ Resilient Formations

How do we calibrate our Force Posture appropriately? How do we work with our allies and partners to capitalise on our different strengths in ways that can challenge Red's thinking, both in competition and conflict? Our goal is to compete effectively; if we are able to do this, the likelihood of going to armed conflict is much less. Although nothing is guaranteed, we can certainly provide our senior national command authority leaders and our coalition leaders options that they currently don't have.

Calibrate Force Posture

Our intelligence community have told us that China and Russia, in particular, have calculated, within the ranges of different types of power and domains, what they think they need in various situations in order to reach their strategic ends. We naturally asked the follow-up question: what is it? The intelligence community went on to say that they weren't fully sure, but that we understand enough about them to know that's how they think. Therefore, whatever we come up with needs to be greater than whatever they have and are planning. Importantly, it's not just about conventional force, although most military folks think that way. But this is much larger than just the military.

When I talk to U.S. Army leaders, we typically think about Forward Positioned Forces. For example, to meet the threats to the Baltics, we can put three U.S. Army Corps somewhere in Eastern Europe. However, there are two problems with that: firstly, it is a political problem. Secondly, the U.S. Army is not growing that big any time soon – we only have three corps, and they have global commitments. Our solution, therefore, has to account for what we call the 'Why Factor' – what is reasonable, and what slight modifications and combinations need to change to be forward postured? And most importantly, we must fully consider how to tie in with our partner forces that are already there, and who already understand and study the adversaries every day.

In addition, we need to ask ourselves how to rapidly penetrate and gain freedom of access into an A2/AD-environment. How do we practise this with our

allies? The X-factor, however, is how to bring in space, cyberspace and information capabilities in ways that we haven't in the past. On this point, the U.S. Army is behind, and we're learning from the U.S Air Force and U.S. Navy which have operated in these areas more effectively for a longer time than the U.S. Army has, because of the threats they have been dealing with.

In summary, we have to calibrate our force posture to meet the threats in a reasonable way, and we ought to present options to both our military and civilian leaders about how we can both compete with, and if needed, fight the enemy and win.

Convergence

How do we break the enemy's campaign plan? We need to converge the capabilities across the domains – space, cyberspace, air, land, maritime, electromagnetic spectrum, and information. Although domains must be used appropriately and not be overused, it helps to account for both Blue's and Red's capabilities across the domains. Friendly forces converge across domains, functions, and environments to create physical, virtual, and cognitive windows of advantage that enable cross-domain semi-independent manoeuvre. This, in turn, to create multiple dilemmas, enables the development and exploit of options, or the dislocation and defeat of enemy systems. The goal is to achieve the friendly operational end state and defeat of the enemy's campaign.

The big challenge in executing Multi-Domain Battle is the ability to master time requirements across domains. A broad example is the lengthy development time of cyber weapons, often taking months, if not years, to develop and deploy. In the land domain, ground forces can take weeks to get to the battlefield, and days to deploy once they are in the area. The battle, however, may be over in a few days, even a few hours. How, then, to mesh those time elements together? Across the Joint Force and partners, we need to sharpen how we think about time, and how we converge our different capabilities for a specific event to give the Blue force, including coalition partners, an advantage over our adversary. How do we give the commander options that put Red on his heels, in both competition and conflict? The aim is to give us the advantage, whether we do it physically, cognitively, or virtually, by manoeuvring in ways which take their campaign plan apart. Our principle is that we want to master and extend time, and make time our advantage, not theirs – to ensure that the coalition has time to organise and build power, both politically as well as militarily.

Summary

Our enemy have expanded the battlefield in four ways – geographically, time, domains, and actors. There are five problems that MDB has to solve, and there are three components to the solution – calibration of force posture, resilient formations, and convergence. The two big ideas that we think are different, not just for the U.S. Army, but for the Joint Force and partners as well, is how to compete effectively, and how to converge capabilities to achieve the one main goal: to break Red's campaign plan in both competition and conflict.

Digitale sårbarheter

av Olav Lysne

For hundre år siden så verden helt annerledes ut. Post levert via hest og kjerre var det vi hadde som tilsvarte internett. Nå har vi de samme tjenestene utført med høyteknologisk utstyr som nettbrett og smarttelefoner. På denne tiden har det skjedd en hel rekke ting med de aller fleste av oss. Blant annet har vi blitt fremmedgjort for hva som kan gå galt, og hvordan vi behøver å sikre oss. Når noen vil forklare dette for oss, vil vi ofte ende opp i en situasjon hvor vi rett og slett ikke forstår hva som blir fortalt. Det tror jeg de aller fleste kan kjenne seg igjen i.

Om man skal forklare de digitale sårbarhetene for sivilsamfunnet, som i hovedsak har vært min beskjeftigelse, er det sjelden at det nytter å forklare teknologiene som gjør en smarttelefon mulig, eller de fysiske fenomenene som har tillatt oss å bygge slikt utstyr i utgangspunktet. Istedenfor ber jeg deg tenke over følgende situasjon: Du er på vei inn i en kiosk og skal kjøpe en bagett. Du tar frem mobiltelefonen, slår den borti kassa, og dermed er bagetten betalt. Det jeg ber deg reflektere over, er alle de involverte virksomhetene som får en slik tjeneste til å virke.

Én virksomhet har laget applikasjonen, for eksempel Vipps. En annen virksomhet har laget telefonen, for eksempel Samsung, Huawei eller Apple. Men for at telefonen skal virke, må den snakke til en basestasjon, som involverer et tredje selskap – i Norge Telia eller kanskje Telenor. På det stadiet er det lett å tro at man er inne i nettverket, men det er litt mer komplisert enn som så. Basestasjonen virker bare hvis den er koblet til en kabel som er eid av en regional nettleverandør. Ut fra det ordet forstår man at det naturligvis finnes en nasjonal nettleverandør som knytter hele landet sammen, og for alle praktiske formål er det Telenor i Norge. De har et kjernenett som kobler sammen alle regionale nettverk.

Vi var på vei fra mobiltelefonen til banken, ettersom det skal utføres en betaling. Da må vi fra kjernenettet ut til en ny regional nettleverandør før signalet kommer til bankens server. Deretter går betalingen mellom to banker – som betyr at bankens server må snakke med den andre bankens server. Det skjer ved at signalet sendes igjen gjennom en regional nettleverandør, til den nasjonale, for igjen å gå gjennom en regional nettleverandør før vi kommer til bank-

tjeneren i den andre banken. Til nå har vi elleve steg som signalet må gjennom.

Men det stopper ikke her. Ettersom man må autentisere seg for å utføre en slik betaling, behøver man BankID eller kodebrikke. Hver av disse to bankene har egne verdikjeder som står for autentisering, begge omtrent like komplekse som gjennomgangen over. Videre er det slik at alle disse tjenestene er levert av private virksomheter, som gjør det private virksomheter gjør – de finner ut hvor de kan skape verdier og tjene penger. Det som ikke er i en privat virksomhets kjernevirksomhet, typisk IT-drift, outsources.

Det betyr at den enkle operasjonen som du gjorde – du skulle jo bare kjøpe en bagett –, involverer tjue–tretti virksomheter. De aller fleste blir overrasket over hvor komplekse digitale verdikjeder som denne faktisk er. Men verdikjeder er ikke noe nytt – hvis man kjøpte en bagett i en kiosk på 70-tallet, ville det fremdeles vært sånn at en bonde måtte ha vært involvert for å lage kornet. Bonden måtte hatt en traktor, og traktoren måtte hatt diesel. Dieselen måtte hatt et raffineri, som måtte hatt en oljepumpe i Nordsjøen. Ergo hadde det samme bildet på sett og vis vært der, men noe har blitt helt annerledes. Det er at i det øyeblikket noe går galt i en digital verdikjede, treffer det de kritiske samfunnsfunksjonene, slik som matleveranse eller betalingstjenester, i samme millisekund. Slik var det ikke før. Hvis det var problemer med å skaffe diesel, tok det litt tid før bonden fikk problemer med å dyrke mat. Det har vi mistet – nå er det altså et millisekund fra noe går galt et eller annet sted i en digital verdikjede, til det treffer kritiske samfunnsfunksjoner. Det er enda en side ved dette: Det er ikke sånn at han du kjøpte diesel til traktoren din av, fikk vite hvem det var som skulle spise bagetten til slutt. Sånn var det ikke før, men sånn er det langt på vei nå. All informasjon om hva som faktisk skjedde i løpet av verdikjeden, blir med langs hele verdikjeden.

Grenseløse verdikjeder

Mitt innlegg skal handle om internasjonale forhold, men så langt har jeg bare viet tid til ting som foregår i Norge. Samtidig er det slik at disse digitale verdikjedene hopper over landegrenser som om de ikke eksisterte. Som en liten illustrasjon kan man tenke over da Helse Sør-Øst vurderte å outsource IT-driften sin til Bulgaria. Hvordan ser da Helse Sør-Østs digitale verdikjede ut når signalene skal sendes til et land som ligger helt i ytterkanten av Europa? Den vil helt opplagt inkludere både virksomheter og utstyr i Sverige, Danmark, Tyskland, Polen, Slovakia, Ungarn og Romania før vi kommer til Bulgaria – i

beste fall. Hvilken vei disse dataene tar mellom Norge og Bulgaria, er det ikke én enkelt virksomhet som bestemmer. Hvert hopp bestemmer neste hopp selv, så det varierer. Etter å ha målt dette ser vi at den stort sett følger den nevnte veien, men av og til går den langt lenger vest, og andre ganger går den gjennom Ukraina og Hviterussland. Samtidig har vi målt øyeblikk hvor verdikjeden går innom Kina, av forskjellige årsaker som er lite transparente for oss.

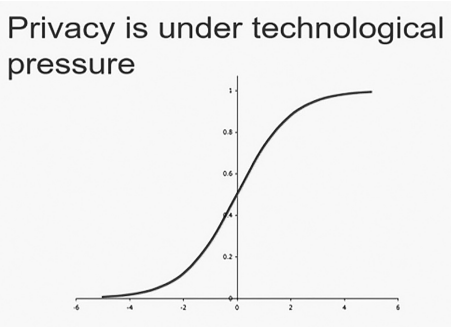
Men dette er altså situasjonen. Videre er det slik at Helse Sør-Øst ikke er de eneste som driver med dette. Svært mange offentlige og private virksomheter er i gang med å outsource IT-driften til forskjellige land rundt om i verden. I Europa er det mye IT som outsources til Irland, mens mye også går til India. I tillegg er det svært mye som outsources til USA. Da kan man reflektere over hvordan verdikjedene ser ut – hvilke land ligger for eksempel mellom Norge og India? Hvem er det vi eksponerer oss for, og hvilke typer utstyr har de?

Svært mange av disse digitale verdikjedene er ikke transparente. Vi vet rett og slett ikke hvordan de ser ut, og det er grunnen til mange av overraskelsene vi har fått – for eksempel nyhetene om at deler av nødnettet ble driftet fra India. Det stemmer, men det visste altså ikke nødetaten selv. Det er en mangel på transparens rundt disse forholdene som gjør at det er svært mye man simpelthen ikke vet. Men det vi skal være klar over, er at nesten alle land eksponerer store samfunnsverdier for andre land, på måter som ikke er transparente. Når man diskuterer begreper som hybrid krigføring, er det verdt å reflektere over akkurat dette.

Digitalt grenseforsvar (DGF) – «Lawful Interception of Internet Traffic in Norway»

Grovt sett er digitalt grenseforsvar en innretning som er ment å gi norsk etterretningstjeneste tilgang til etterretningsinformasjon hentet ut av de internettkablene som går inn og ut av Norge – et grenseforsvar, men digitalt, som henter ut de digitale strømmene som krysser landegrensene.

I lys av det bildet jeg har presentert innledningsvis, fremstår det som opplagt at vi må ha dette. Vi er nødt til å hente etterretningsinformasjon ut av det digitale rom. Vi gir jo etterretningstjenesten oppdrag i det digitale rom; de er nødt til å gjøre noe der, og det er et opplagt sted for dem å være. Mange vil nok lande på dette standpunktet. Samtidig er det ganske sterke strømninger i samfunnet som er motstandere av et digitalt grenseforsvar. Hva er motstandernes argumenter?



Det skal jeg forklare ved å begynne med «S-kurven». Den brukes mye i samfunnsvitenskap, økonomi og naturfag for å beskrive endringer. Jeg bruker den for å illustrere en samfunnsendring som kommer som et resultat av en oppfinnelse.

La oss ta oppfinnelsen av radioen som et eksempel – i starten beveger ikke kurven seg. Deretter begynner man å forstå litt mer om hva radioen kan brukes til. Det gikk an å produsere den billigere, og flere kjøpte en radio. Dermed skyter kurven fart. Etter hvert nådde radioen en stabil tilstand hvor hele oppfinnelsens potensial for samfunnsendring hadde blitt tatt ut. Når det gjelder digitalt grenseforsvar og personvern, som er det sentrale begrepet når man skal forstå motstanderne av digitalt grenseforsvar, er det to fenomener som for øyeblikket er på vei oppover i denne kurven. Det ene er lett å forklare – hvilken informasjon som blir digitalisert om hver enkelt av oss. Hvilken personlig informasjon om meg er det som blir digitalisert og sendt gjennom disse kablene?

Mitt liv i dag: Jeg sto opp halv seks, siden jeg skulle fly klokken åtte. Jeg fikk raskt sjekket e-posten før jeg tok meg en kopp kaffe. Deretter løp jeg ut og tok bussen til Nationaltheatret, hvor ferden gikk videre til Gardermoen med tog. Deretter tok jeg fly opp til Trondheim og ble kjørt av en kadett til Luftkrigsskolen. Underveis på turen sjekket jeg tidvis e-post og forberedte meg til min presentasjon. All denne informasjonen om mitt liv er blitt digitalisert. Slik informasjon vil krysse de norske landegrensene etter kort tid, senest når telefonen min gjennomfører en automatisk backup. Hvorfor det? Jo, fordi den digitale verdikjeden til backup-funksjonen på telefonen min, en iPhone, går til Apple i USA.

Dermed er det slik at den informasjonen som vi alle sammen veldig gjerne vil at etterretningstjenesten skal få tak i for å gjøre sitt viktige oppdrag på vegne av oss, bader som små dråper i et hav av informasjon om hver enkelt av oss.

Det andre som er på vei oppover i kurven, er stordatanalyse. For dem som

ikke er teknologer, kan det muligens være et hemmelig og rart ord. Men for å illustrere det kan jeg komme med et eksempel: Jeg vet fire ting om en kvinne – hun er 30 år, hun er barnløs, hun var hos legen sin på torsdag, og hun så på en leilighet på søndag. Det er ikke så mye informasjon om henne da, men det kan spore til en refleksjon over lunsjbordet om hun kanskje er gravid. Man kan deretter legge til litt mer informasjon – at hun er registrert som å være i et forhold på Facebook, og at hun akkurat har byttet jobb fra en utsatt jobb i privat sektor til en lærerjobb. For hvert tillegg av slike detaljer vet man at sannsynligheten for at hun faktisk er gravid, øker. Slike ting kan være artige å snakke om rundt lunsjbordet, men det som ligger i stordatanalyse, er at det ikke lenger er begrenset til lunsjbordet – nå kan det regnes ut. Det regnestykket har dessverre blitt så stygt at dersom man kjenner en åtte–ti slike detaljer, behøver man ikke lenger lure på om man har regnet riktig. Da ligger nemlig ikke usikkerheten i regnestykket, men i nøyaktigheten på graviditetstesten. Dette forandrer bildet ganske kraftig. Ut fra forhold som overhodet ikke har noe med hennes graviditet å gjøre, kan man altså med stor sikkerhet slutte seg til hvorvidt kvinnen er gravid.

Personvern

Dette underbygger motstandernes argumentasjon i kritikken mot DGF. Det de er redde for, er at eierskapet til informasjonen om en selv er på vei til å forsvinne. Dette leder til flere nye spørsmål: Hva vil være teknologisk mulig om 20 år? Det vet ingen. Vi er derimot på vei inn i en tidsalder hvor det å overvåke samtlige borgere i et land, hver time hvert døgn hele året, er teknologisk og økonomisk mulig – og ikke engang spesielt vanskelig. Og hva vil være regnet som kompromitterende informasjon om 20 år? Vil det være mulig å tillate innsamling av store datasett, og senere forby det? Burde vi bekymre oss for at uvedkommende skal kuppe kontrollen over slik datainnsamling? Hvor sterk er den såkalte «chilling»-effekten?

På grunn av disse usikkerhetsmomentene er spørsmålene om et digitalt grenseforsvar ekte, vanskelige spørsmål. Vår generasjon er den som utsettes for valget – hva gjør man med dette? Det finnes en stor gruppe mennesker som mener at spørsmålet er enkelt. Det interessante med disse menneskene er at de deler seg i to, og de to grupperingene er dundrende uenige med hverandre. De eneste jeg er dundrende uenig med i denne diskusjonen, er de som insisterer på at det er enkelt. Det er det ikke, og de som mener det er enkelt, tar feil.

«Does Lawful Interception Break the European Declaration of Human Rights?»

Jeg har ledet et utvalg som konkluderte med at vi bør innføre et digitalt grenseforsvar. Jeg skal si litt om hvorfor vi landet på den beslutningen. Men først: Det som synes å være det avgjørende elementet når DGF skal opp til behandling i Stortinget etter sommeren 2018, er hvorvidt DGF bryter med den europeiske menneskerettskonvensjonen eller ikke. Personlig mener jeg at DGF ikke gjør det, men det er likevel et godt spørsmål. Den europeiske menneskerettskonvensjonen er skrevet i en tid da man ikke hadde datamaskiner, og nå prøver man å forstå hva den egentlig betyr i den digitale tidsalderen. Det er svært få klare svar å få ut av dette, men det sildrer en og annen kjennelse ut av Strasbourg som gjør at man kan få et litt bedre grep om hva det er snakk om.

Men fra disse punktene skal jeg gå over til resonnementet som gjør at jeg mener at vi må ha et digitalt grenseforsvar i Norge. Det er nemlig slik at vi ikke kan slutte å gi etterretningstjenesten oppdrag å løse i det digitale rom. Grunnen til det er at det digitale rom har blitt altfor viktig – det styrer all kritisk infrastruktur i Norge, slik som vannforsyning til de store byene og strømleveranser til hele befolkningen og til våre institusjoner, for eksempel sykehusene. Hvis det slutter å virke, vil tog stoppe og fly stå på bakken. For ikke å snakke om kriseledelse – hvis hele kjernenettet vårt dør, er ansikt til ansikt den eneste måten å kommunisere med folk på. Det er ikke samfunnet vårt tilrettelagt for. Hvis vannforsyningen i Oslo stopper, skal byen evakueres etter seks timer. Det er verdt å reflektere over hvordan det kan gjennomføres hvis den eneste kommunikasjonsformen man har, er ansikt til ansikt, samtidig som alle T-baner og trikker står stille. Det ville ikke vært enkelt.

Vi kunne kanskje fortalt etterretningstjenesten hvor de skulle oppholde seg i det digitale rom, og funnet steder hvor de finner informasjonen de trenger, og som samtidig er frie for personopplysninger. Men som teknolog vet jeg at de stedene ikke finnes. Noe av det vakre med elektronisk utstyr og datamaskiner er at de kan brukes til alt mulig rart. Dette har dere opplevd selv med smarttelefonen – man kan laste ned en ny app, og plutselig har det blitt et helt nytt verktøy. Det samme prinsippet gjelder med den digitale infrastrukturen – den kan brukes til alt. Det betyr at det er den samme infrastrukturen som brukes til absolutt alt. Det er ikke noen steder i den digitale infrastrukturen hvor man kan si til etterretningstjenesten at det er fritt for personopplysninger.

Som følge av dette, og så lenge vi er nødt til å gi etterretningstjenesten oppdrag å løse i det digitale rom, må de ha tilgang til steder hvor informasjonen de

skal ha tak i, svømmer i et hav av personopplysninger. Sånn er det. I tillegg er det slik at alle nabolandene våre har innført digitale grenseforsvar. Storbritannia og Sverige har innført det og er åpne om det, mens Finland er i ferd med å innføre det. Gjennom Snowden-lekkasjene kom det frem at Danmark også nok har gjort det, uten at de er åpne om det. Og det er vel ingen som tror at Russland ikke driver med dette? Alle grensekablene som går ut av Norge, går jo gjennom disse landene. Det betyr at vi er overvåket, men ikke av norsk etterretning.

Vi må derfor gi dem tilgang i det digitale rom. Den eneste måten vi kan gjenvinne en form for kontroll med personvernet i en slik situasjon på, er å begrense hva de har anledning til å hente ut, og hva de får lov til å bruke informasjonen til. Og så må vi ha kontrollmekanismer som sikrer at de holder seg innenfor disse grensene. Jeg mener at det er den eneste farbare vei fremover. Det farligste vi kan gjøre, er å stå stille der vi er nå – hvor vi nekter etterretningstjenesten tilgang til det digitale rom, samtidig som de får oppdrag de må løse der.

Kritisk infrastruktur

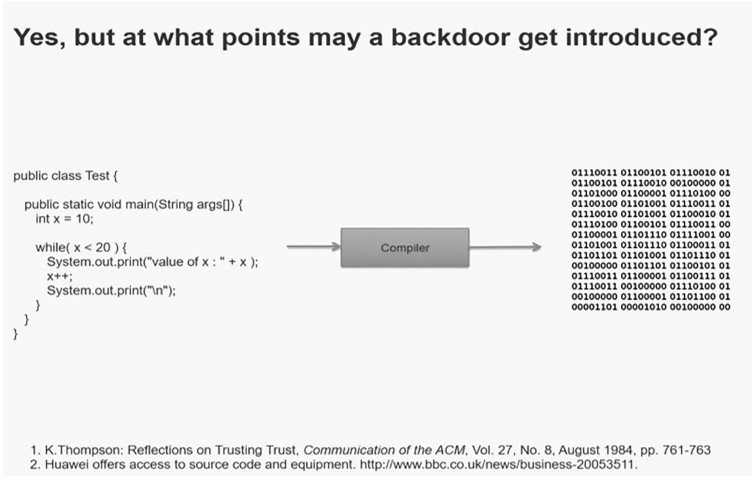
Huawei er et stort, kinesisk telekom-selskap som i løpet av de siste ti–femten årene har vokst til å bli en av verdens største leverandører av utstyr til kritisk infrastruktur. Da de fikk fart i salget til vestlige land, kom det opp en hel rekke diskusjoner om det er noe vi skulle tørre å kjøpe. De diskusjonene fikk mange ulike utfall i forskjellige land. Noen land forbød det. Andre land, som Norge, sa ja. Derfor vil de fleste basestasjoner i landet være produsert i Kina av Huawei. Det er riktignok slik at Norges ja til dette kom gjennom sammenbitte tenner, fordi man lette etter lovhjemler som tillot å forby det. Dette var imidlertid ikke på plass.

Diskusjonen var likevel enkel. Lenge gikk den mest ut på hvorvidt vi skulle tørre å kjøpe kinesisk eller ikke. Men så kom Edward Snowden på banen og rotet til diskusjonen. Det er mange diskusjoner rundt kinesiske selskaper, men de har aldri blitt tatt i å gjøre noe galt. Fra dokumentene som Snowden friga, kom det tydelig frem at det er amerikanske selskaper, for eksempel Cisco, som har blitt satt i situasjoner hvor de må lekke informasjon tilbake til de hemmelige tjenestene i USA. Det forrykket den norske diskusjonen, og spørsmålet om hvorvidt Norge, et lite land, skal forby import av digital infrastruktur fra både Kina og USA, meldte seg. Det ville blitt en interessant infrastruktur. Selv har jeg en svært dårlig håndskrift og har lite lyst til å gå tilbake til den. Men det er tilbake til håndskriften vi i så fall må. Siden Norge er et lite land, er det sånn at vi enten må kjøpe fra et land vi mistenker for overvåkning gjennom digital infrastruktur, eller fra et land som har blitt tatt i å gjøre det.

I Volkswagen-skandalen laget ingeniører en chip som oppdaget når den skulle bli testet. Denne ble så installert i dieselmotorer. Det fikk motoren til å oppføre seg annerledes ved testing; den slapp ut mindre av gassen nitrogenoksid (NO_X). Med andre ord oppførte den seg annerledes på veien enn i testsituasjoner. Det interessante med dette er at ingeniørene kunne gjøre dette i trygg forvissning om at en slik elektronisk chip ikke lar seg analysere til bunns. Denne situasjonen er vi nødt til å ta inn over oss – i det øyeblikket vi kjøper elektronisk utsyr fra en eller annen leverandør, er vi henvist til nærmest blind tillit til at de har bygget utstyret på en måte som hindrer det i å operere mot vårt ønske.

Kjernespørsmålet vi må stille oss, er derfor hva vi som et lite land kan gjøre når vi samtidig er nødt til å kjøpe utstyr til vår kritiske digitale infrastruktur fra folk vi ikke nødvendigvis stoler fullt og helt på? Dette bildet gjøres svært komplekst av at nesten alt av utstyr, inkludert de fleste mobiltelefoner, består av komponenter som er laget i USA og Kina. Det er svært lite elektronisk utstyr som er laget helt og holdent i ett land.

Grunnen til at det er vanskelig å undersøke digitalt utstyr, er at det er en svært komplisert øvelse. Dersom du har programmert, vil du kjenne igjen programmeringsspråket til venstre på bildet under. Om du ikke har programmert, ville jeg med letthet kunne forklare, grovt sett, hva koden gjør. Det er dermed et eksempel på noe som er forståelig for et menneske. Men det som kjører på datamaskinen, er koden som utelukkende er satt sammen av 0 og 1, og den er langt mindre forståelig for et menneske. For å oversette mellom de to språkene, fra det et menneske kan forstå og skrive, til noe en datamaskin kan utføre, benyttes en kompilator.



Dermed kan alle mulige bakdører, for eksempel i elektronisk utstyr, installeres ved hjelp av en kompilator. Selv i det tilfellet at jeg som kjøper bruker et eget team som overvåker ingeniørene mens de lager det elektroniske utstyret jeg skal bruke, vil det ikke bli oppdaget at en bakdør har blitt installert. Ingeniørene ville ikke nødvendigvis visst om en bakdør, de heller, da den kunne ha blitt installert via et av verktøyene som ingeniørene brukte.

Det betyr at vi er i en situasjon vi aldri har vært i før – vi kan ikke lenger kjøpe utstyr og plukke det fra hverandre for å se hva det gjør, slik at vi kan forsikre oss om at det er trygt. Den tiden er forbi. Straks vi kjøper elektronisk utstyr som involverer verdikjeder vi ikke har kontroll på, må vi stole ganske blindt på hva det utstyret faktisk gjør.

Dette er faktaene

1 Når en ukjent tredjepart er fienden, finnes det metoder som, når de er korrekt implementert og profesjonelt utført, gjør det vanskelig og ressurskrevende å bryte inn i et system uten å bli oppdaget.
2 Når leverandøren av utstyret er fienden, finnes det tilsynelatende ingen metoder, selv ikke om de er profesjonelt utført, som har signifikant effekt på våre evner til å forebygge eller oppdage skadelige handlinger.
3 Heterogenitet i infrastrukturen og sterk kryptering fra ende til ende fremstår som den eneste muligheten fremover.

Dette innlegget har noe utilfredsstillende ved seg, ved at jeg kaster en hel rekke problemer opp i lufta uten å ta dem ned igjen. Vanligvis vil man i tilsvarende innlegg presentere et problem, en analyse og en løsning på problemet. Med dette innlegget ønsker jeg å bevisstgjøre om hvordan verden faktisk ser ut – om at vi faktisk har en dyp kompleksitet knyttet til digitale verdikjeder som gjør at svært mange land har eksponert seg digitalt for mange andre land, ikke minst med hensyn til sin kritiske infrastruktur. Videre tror jeg vi skal slutte å tenke at norsk kritisk infrastruktur ligger i landet; det er det slettes ikke sikkert at den gjør. Men situasjonen er slik at måten vi beskytter oss på, er under utvikling. Den digitale verdenen har utviklet seg fra å være et leketøy på 1980-tallet til å bli helt sentral i kritisk infrastruktur. Denne prosessen har skjedd gradvis, uten at noen deler av samfunnet egentlig har hengt med, heller ikke utdanningsinstitusjonene. Som samfunn står vi derfor og vipper på hælene og forsøker å komme oss tilbake i balanse.

Disse faktaene må danne rammebetingelsene for alle beslutninger vi tar. Jeg ønsker, spesielt i forumer som dette, hvor begreper som hybrid krigføring duk-

ker opp, at man skal ha en vesentlig større klarhet i hvilke samfunnsverdier man faktisk har eksponert for hverandre digitalt, enn det som er tilfellet nå. Jeg er ikke så godt kjent med Forsvaret, men jeg er svært godt kjent med elektronikk og infrastruktur. For meg ser det ut til at det er fullt mulig å slå Norge av fra utlandet – for eksempel stoppe vannforsyningen og kraftleveransen til byene, stoppe all elektronikk i sykehus, stoppe alt av kriseledelse, sette fly på bakken og stoppe togene – helt samtidig, uten å løsne et skudd. Et slikt scenario ville fått dødelig utfall.

Det er andre enn meg som best vurderer hva som egentlig ville skjedd i et land om dette hadde inntruffet og landet deretter ba om forhandlinger. Hybrid krigføring er en del av bildet, men ren digital krigføring, det å overta et land med digitale midler, fremstår som mulig. Dette scenarioet skulle jeg ønske var mer fremtredende i forumer som dette.

Teknologi og fremtiden fra en kadetts perspektiv

av Eva Johanne Merkesdal

Temaet for årets luftmaktseminar, *Multi-Domain Battle* (MDB), var for meg et ukjent begrep. Min første respons var derfor å gjøre et raskt Google-søk. Så, hva er egentlig Multi-Domain Battle? Multi-Domain Battle et er ferskt konsept innen krigføring som er utviklet for at vi skal være fellesoperative og ha mulighet til å operere synkront i de ulike domenene – hær, sjø, luft, cyber og space. Å være fellesoperativ er ikke noe nytt, men både cyber og space er hurtigvoksende domener som vil ta mer plass i det fellesoperative bildet. Multi-Domain Battle blir vesentlig om man kjemper mot en fiende som er tilsvarende en selv teknologisk. Slik jeg ser det, handler Multi-Domain Battle om en ny og høyaktuell måte å føre krig på, med høyere integrering av cyberforsvar og space. Med ny teknologi i stadig utvikling åpner det seg uante dører for hvordan krigføringen blir i fremtiden.

I denne artikkelen vil jeg rette søkelyset mot nettopp det: fremtiden og teknologi. Jeg vil se på hvordan ny teknologi former en moderne slagmark med utfordringer vi ikke har sett før. Jeg vil i første omgang rette oppmerksomheten mot cyber, og her vil jeg fortelle om Stuxnet, et virus som angrep i 2010. Deretter vil jeg vende blikket mot svermteknologi og hvordan krigføring har tatt en uventet vending ved bruk av droner. Avslutningsvis vil jeg presentere tre egne synspunkter som jeg mener blir viktig å ta i betraktning på vår ferd mot å bli et moderne multidomeneforsvar.

Cyberkrigføring – fienden man ikke ser

Når ny teknologi kommer på banen, åpnes det for nye måter å føre krig på. Det er ikke så enkelt å spekulere i hvordan fremtidens slagmark kommer til å se ut, men jeg tror at IKT kommer til å ta mye større plass i fremtidens krigsscenario enn det gjør i dag. Fremtidens slagmark kan komme til å bli så kompleks at vi trenger bedre situasjonsbevissthet og bedre kontroll over hva som foregår i operasjonsområdet. IKT danner grunnlaget for at Forsvaret skal fun-

gere i det daglige, i krig, i fred og i fellesoperasjoner, og det er Cyberforsvaret som driver Forsvarets ressurser innen informasjons- og kommunikasjonsteknologi. Cyberforsvaret er en raskt voksende del av norsk militærmakt, og det er viktigere enn noen gang å beskytte seg mot datatrusler. Jeg er ingen teknolog, ei heller ansatt i Cyberforsvaret, men cyber er noe som fascinerer meg. Cyber er gjerne det domenet og den våpengrenen man generelt ikke har så mye kunnskap om eller kjennskap til, og så lenge computerne og kommunikasjonssystemene fungerer, er det ikke alltid man tenker over eller legger merke til Cyberforsvaret. Jeg opplever også at flere mangler generell kompetanse i dette domenet. For å beskrive dette på en annen måte ønsker jeg å ta i bruk to begreper: *digitalt innfødte* og *digitale immigranter*.

Dagens ungdommer kan betegnes som digitalt innfødte; de er vokst opp i en tid hvor mobiltelefoner, internett og computere alltid har eksistert og oppleves som helt normale hjelpemidler i hverdagen. De digitalt innfødte surfer seg gjennom cyberspace og bruker gjerne internett og datamaskiner på en ukritisk måte. På den andre siden har man de digitale immigrantene, som kan betegnes som den eldre garde eller den eldre generasjonen. Denne gruppen mennesker gikk gjerne gjennom universitetsutdannelsen sin uten å ta i bruk en eneste computer, og fra deres perspektiv er internett noe som plutselig dukket opp, og som mennesket trengte tid for å venne seg til. For dem kan internett gjerne virke forvirrende og unaturlig. Flere av våre eldste og mest erfarne ledere har begrenset erfaring med computere og internett.

Problemet jeg forsøker å komme frem til her, ligger verken hos de digitale immigrantene eller hos de digitalt innfødte, men i spekteret og avstanden mellom dem. Cyber har på mange måter sitt eget språk som det kreves tid og kompetanse for å forstå. Data er lagret virtuelt og ikke fysisk. Dette gjør cyber abstrakt og til en av de mest komplekse områdene. Selv tilhører jeg gruppen digitalt innfødte, men teknologien utvikler seg i en så høy hastighet at jeg sliter med å holde følge. Lillesøsteren min har allerede tatt meg igjen på dette området selv om aldersforskjellen mellom oss kun er tre år. Dette sier litt om hastigheten teknologien utvikles i. Det er ikke noe annet domene som har utviklet seg så hurtig som cyber, og cybersikkerhet blir viktigere enn noen gang før. Allikevel er det de færreste som forstår seg på dette domenet – men alle forstår at de burde forstå.

Stuxnet

For å illustrere hvor mulighetsrike, men også hvor sårbare cyber, internett og computere kan være, ønsker jeg å trekke frem et eksempel fra 2010 hvor 200 000 computere verden over ble infisert av et virus som ble kalt Stuxnet.

Viruset var ikke ute etter å angripe vanlige computere, men hoppet mellom computere og minnebrikker på jakt etter en spesiell enhet som var lokalisert i Iran. Dataormen var programmert til å angripe SCADA[1]-systemer, systemer som brukes til overvåkning av industrielle prosesser (Friedman, 2014). I Iran var de i full gang med å anrike uran. Uran er et radioaktivt grunnstoff som blir brukt i produksjon av blant annet atomvåpen og atombrensel. Iran insisterer på at landets atomprogram kun har fredelige formål, men vestlige stormakter frykter at landet i skjul har planer om å utvikle atomvåpen. Det var dermed interesse for å stoppe denne produksjonen.

Det som gjør dette viruset annerledes og mer sofistikert enn andre virus, er at computere ikke viste noe tegn til at de var infisert av et virus. Vi forventer at en computer skal varsle oss om sin nåværende situasjon. Når de ikke ble varslet, var dermed ingeniørene som arbeidet inne på uranutvinningsanlegget, helt uvitende om funksjonsfeilene dette viruset var i ferd med å forårsake. Viruset var programmert til å skjule endringer og å slette spor etter seg selv. Det angrep PLS-systemet[2] , altså styringsenheten i sentrifugene, en kritisk komponent i anrikingen av uran. Viruset var programmert til først å øke hastigheten på sentrifugene, og deretter til å senke det og igjen øke det. Dette førte til at sentrifugene gikk i egenresonans og vibrasjonene ødela maskineriet.

Dette eksempelet viser et offensivt angrep gjennomført fullt og helt i cyber, uten at et eneste menneskeliv gikk tapt. Dette angrepet hadde gjerne ikke vært like aktuelt å gjennomføre med luftangrep, da produksjonen inneholdt eksplosiver og konsekvensene kunne vært fatale. En annen faktor er at Iran kunne ha sett på dette som en krigserklæring. Angrepet ble derfor gjort i full hemmelighet.

Et virus har innebyggede koder; man kan på mange måter se på disse som virusets DNA. Ved å studere dem kan man finne tegn på hvor viruset er laget. Stuxnet-viruset var svært avansert og skiller seg helt fra andre virus vi kjenner til. Man vet fortsatt ikke med sikkerhet hvor dette viruset har sitt opphav, men det spekuleres i om USA har hatt noe med dette offensive cyberangrepet å gjøre.

Grunnen til at jeg ville trekke frem dette eksempelet, er at det illustrerer mulighetene som ligger i cyber til å sabotere og forstyrre infrastruktur, samtidig som det viser hvor sårbar man er mot sofistikerte cyberangrep. Alle trenger ikke å vite alt om Stuxnets programmeringskoder eller eksakt hvordan et virus

1 Supervisory Control and Data Acquisition
2 Programmerbar logisk styring

angriper, men jo mer avhengig man blir av denne teknologien, jo større generell forståelse av systemene bør man ha. Her ser jeg et forbedringspotensial i Forsvaret i dag. Med et voksende cyberforsvar blir forståelse av cyberdomenet enda viktigere. Dette gjelder enten man er digitalt innfødt eller digital immigrant.

Både Forsvaret og sivile har gjort seg avhengige av systemer som man egentlig ikke vet hvordan fungerer, og som man til tider gjerne tar for gitt at skal fungere. For hva vil skje dersom man plutselig en dag ikke har et fungerende nettverk, internett, Fisbasis, IMAS, SAP, NECCIS, ALIS, Link og så videre? Det hadde vært interessant å se hvor lenge Forsvaret hadde klart seg uten nettverk. Nettopp det å fungere og å operere uten nettverk er noe vi burde trent enda mer på i øvelser, og det er fordi det er den avanserte teknologien som gjerne er det første som svikter når krigen bryter ut. Det er her de digitale immigrantene kommer inn i bildet igjen. Den eldre generasjonen må da trå til med gårsdagens manuelle ferdigheter og vise oss digitalt innfødte hvordan man opererer uten nettverk og datamaskiner. Dette kunne vi digitalt innfødte helt sikkert trengt mer trening i.

Til ettertanke: Stuxnet-viruset angrep PLS-systemer, altså styringsenheter. Samfunnet rundt oss er styrt av PLS i alt fra enkel lys- og varmestyring til større produksjoner og i prosessanlegg som for eksempel vannforsyningsanlegg, jernbanenett, trafikklys og kraftverk. Er staten Norge godt nok beskyttet mot virus og hacking som kan angripe styringssystemene våre? Og vet vi egentlig nok om skadelig programvare?

Se for deg at elektrisiteten blir borte – tog slutter å gå, lyskryss slutter å fungere, vannforsyningen svikter, bankautomater og datamaskiner bryter sammen. Og kritisk syke pasienter på sykehus får ikke den behandlingen de trenger, siden viktige maskiner bryter sammen. Et slikt scenario er ikke science fiction; det kan bli en realitet som skaper kaos og panikk i befolkningen. Cyberkrigføring er den farligste og største endringen i bruk av militærmidler vi har sett de siste 50 årene, og det er omgitt av et massivt hemmelighold. Det er lite fremme i offentlig omtale og debatt, men datasikkerhet har aldri vært viktigere.

Svermdroner

Man må gjerne ikke bare se begrensningene i det som tradisjonelt har tilhørt våpengrenene, for om man ser i spektrene *mellom* våpengrenene, kan man finne nye måter å føre krig på. Dette bringer meg til det neste fenomenet som jeg vil omtale, nemlig svermteknologi. Slik jeg ser det, er mikrodroner og svermdroner på mange måter i spekteret mellom luft og cyber.

Svermdroner er programmert til å holde en gitt hastighet og avstand og til

å følge et spesifikt operasjonsmønster. Et nettverk av mikrodroner er styrt fra en computer utenfor operasjonsområdet, men innenfor dronenes rekkevidde. Svermteknologi er billig og enkel teknologi med rask reaksjon, høy mobilitet og høy tilgjengelighet. Én sverm kan bestå av omkring tusen droner – denne teknologien er intet annet enn imponerende.

Droner har potensial til å skape mye forstyrrelser og «clutter[3]», men kan også brukes til overvåkning og informasjonsinnhenting, såkalt ISR[4]. Svermdronene kan dessuten ha en «weapons bay» hvor de har mulighet til å lagre mindre eksplosiver. Det som er urovekkende ved svermdroner og denne typen teknologi, er kostnaden. Dette er billig teknologi som kan gjøre det kostnadseffektivt å gå til krig. Krigføring med slike midler kan dermed bli tilgjengelig for grupper med mindre ressurser, og skadepotensialet er enormt.

Vi er vitne til en rivende teknologisk utvikling som åpner for mange muligheter innen krigføring. Forsvaret kan velge om de ønsker å ta i bruk den nye teknologien eller ikke, men vi er uansett nødt til å forberede oss på å måtte kontre denne trusselen i fremtiden. Men hvordan kan man egentlig beskytte seg mot lavtflygende svermdroner? Kanskje vi blir nødt til å bytte ut HK416 med hagler for å ha sjanse til å treffe dronene? Eller kanskje vi er nødt til å gå til innkjøp av CIWS[5]-systemer eller andre nærforsvarssystemer? Laser? Eller hva med en elektromagnetisk puls som kan slå ut elektronikken i de små dronene? Et annet alternativ kunne vært å utvikle anti-drone-droner som kan gå til luftkrig mot fiendens droner, slik at vi etter hvert kunne fått en fullskala robotkrig? Her gjelder det å være kreativ, for per dags dato har vi ingen plattformer som er gode nok til å kunne beskytte oss mot denne trusselen. For å belyse poenget ytterligere vil jeg vise til episoden der en enkel drone til 1660 kroner ble skutt ned med et Patriot rakettmissil til omtrent 30 millioner kroner (Sandberg, 2017). Uttrykket «å skyte spurv med kanon» får plutselig en dagsaktuell og oppdatert betydning. Skal vi kunne kontre denne teknologien, blir vi nødt til å produsere nye og mer effektive våpen. Å bruke missiler til flere titalls millioner kroner er ikke bærekraftig; da bringer vi oss selv til konkurs.

Allerede finnes det flere eksempler på at droner er blitt brukt i krigføring. I januar 2018 gjennomførte syriske opprørsgrupper et stort angrep med hjemmelagde droner mot de russiske basene i Syria. Angrepet resulterte i at fire menn ble drept og flere jagerfly ble ødelagt (Andreassen & Johansen, 2018).

3 Clutter er støy på en radarskjerm som for eksempel kan skyldes skyer eller fronter i atmosfæren. For en uerfaren operatør kan dette mistolkes til å være noe annet enn det i virkeligheten er.
4 Intelligence surveillance and Reconnaissence
5 Close-in weapon system

Dronene var riktignok av enkel oppbygning og karakter. De ble styrt fra et sted 20–30 kilometer unna målet, og de slapp bomber ved hjelp av GPS-koordinater. Som nevnt er droner billig teknolog, det er vanskelig å stoppe spredningen av denne teknologien når selv opprørsgrupper i Syria har skaffet seg den. Luftrusselen i form av lavtflygende droner gjør tradisjonell bruk av luftmakt irrelevant. Man kan ikke bruke jagerfly, ei heller AMRAAM-missiler[6], for å beskytte seg mot droner som flyr i trehøyde. Hvis krig i fremtiden vil føres med kostbesparende våpensystemer, vil det muligens ikke lenger lønne seg å bruke de dyre, overlegne kapasitetene som de store nasjonene innehar i dag (Kristensen, 2017).

Enda mer komplekst blir det om svermdronene i fremtiden utstyres med kunstig intelligens og får muligheten til å operere autonomt. Dronene vil da være i stand til å identifisere og engasjere mål uten at et menneske drar i avtrekkeren. Dette vekker igjen debatten om autonome våpensystemer er etisk og juridisk forsvarlig. Denne debatten er så kompleks og tidkrevende at jeg ikke kommer til å gå dypere inn i den her. Etikken ved bruk av fjernstyrte og autonome maskiner i krigføring er sterkt omdiskutert, da denne teknologien potensielt kan føre til en tredje revolusjon innen krigføring.

Vi er inne i en rivende teknologisk utvikling, og krigføringen er i ferd med å endre karakter. Mot et avansert svermangrep er vi per dags dato sjanseløse. *Svermdroner høres kanskje ut som science fiction, men egentlig er det bare science.*

Fremtiden er fellesoperativ

Jeg mener at Multi-Domain Battle innebærer mye mer enn å skrive en ny doktrine eller å kjøpe inn nytt materiell. Vi har en travel tid foran oss om Forsvaret skal kunne kalle seg multi-domain før vi opererer og fungerer sammen som en enhet, og dette er noe som kommer til å kreve mye tid til opptrening og øvelser. Som vi vet, må man lære seg å gå før man kan løpe, men aller først må man lære seg å krabbe. For å forberede oss mener jeg at vi først bør begynne med de små og enkle endringene. Derfor synes jeg at vi bør begynne med å endre holdninger og kultur før vi etter hvert kan ta på oss de større endringene.

La oss begynne med utdanning og kompetansebygging. For å være fellesoperative trenger vi kunnskap på tvers av grenene, slik at vi kjenner til de ulike avdelingenes muligheter og begrensninger. Vi må også skape relasjoner som legger grunnlaget for fremtidig samarbeid. Utdanningsreformen er noe jeg tid-

6 Advanced Medium-Range Air-to-Air Missile

ligere har vært veldig negativ til, nettopp fordi den rammer en avdeling jeg er blitt glad i. Skal vi være fellesoperative i fremtiden, ser jeg absolutt nytten av å ha offisersutdanningen samlet på ett sted. På denne måten kan man sikre en grunnleggende kunnskap om hverandres våpengrener, og man stifter bekjentskaper på tvers av våpengrenene/domenene, noe som vil bli viktig i fremtidig samarbeid.

Det neste jeg mener vi bør tenke på, er holdninger og avdelingskultur. En sterk avdelingskultur er viktig, men til tider kan denne avdelingskulturen bli så sterk at den virker mot sin hensikt. Å være multi-domain betyr å være fellesoperativ, og det vil si at man må gi slipp på deler av avdelingskulturen og være åpen for å gjøre ting annerledes for å kunne samarbeide bedre. Det må etableres en kulturforståelse og åpenhet ute i avdelingene som forenkler samarbeid mellom ulike avdelinger og våpengrener. En tettere sammenkobling mellom forsvarsgrenene vil jeg si er selve essensen i Multi-Domain Battle.

Avslutning og oppsummering

Jeg har ikke skrevet så mye om hær, sjø og space, som også utgjør en stor del av Multi-Domain Battle, for multi-domain er ikke bare cyber, sensorer og sciencefictionlignende teknologi. Men cyber, nettverk og informasjonsdeling er på mange måter «limet» som kan få Multi-Domain Battle til å fungere i praksis. Skal vi operere fellesoperativt, trenger vi informasjonsdeling og nettverk. Fremtidens krigføring hviler på et fundament av nettverk, og uten dette nettverket vil vi ikke kunne hevde dominans i stridsområdet. Jeg ønsket også å sette Cyberforsvaret i søkelyset, da dette er en nyopprettet våpengren som jeg synes får altfor lite medieomtale og oppmerksomhet. Vi hadde ikke klart oss uten dem.

Jeg har også forsøkt å belyse problematikken rundt svermdroner og skadepotensialet ved denne typen teknologi samt hvor lite beskyttet vi er mot denne trusselen. Ny teknologi former en moderne slagmark som vi ikke har sett før. Datavirus, datasikkerhet og svermdroner gir nye utfordringer som det kan bli krevende å utvikle mottiltak mot.

Jeg vil tørre å påstå at vi befinner oss midt oppi en teknologisk revolusjon. Det er viktig at Forsvaret da ikke sitter på gjerdet, men at vi aktivt tar i bruk den nye teknologien. Dette er nødvendig om vi skal være en seriøs aktør i NATO. Fremtiden er fellesoperativ.

Referanser

Andreassen, T.A. og Johansen, P.A. (2018, 12. januar). En dronesverm kom fullstendig overraskende på de russiske soldatene. Nå må Putin svare på om han tok seieren på forskudd. *Aftenposten*. https://www.aftenposten.no/verden/i/1k7vBl/En-dronesverm-kom-fullstendig-overraskende-pa-de-russiske-soldatene-Na-ma-Putin-svare-pa-om-han-tok-seieren-pa-forskudd

Friedman, P.S. (2014). *Cybersecurity and Cyberwarfare*. New York: Oxford University Press.

Kristensen, P. (2017). *Autonome våpensystemer – krigens frelser eller synder?* Semesteroppgave. Trondheim: LKSK.

Sandberg, H. (2017, 17. mars). Skjøt spurv med kanon. NRK Urix: https://www.nrk.no/urix/brukte-patriot-rakett-til-a-skyte-ned-billig-drone-1.13429562

Adapting to the Cyber Threat

by Lior Tabansky

In the last several years, my research has been focussed on issues addressing national security in its proper sense – protection against foreign, state-sponsored threats. Today, I will discuss the fact that the armed forces in most countries do not perform the basics in cyberspace at the level at which they perform them in other areas. First, countries do not understand or know what is going on in their respective national cyberspace. And more importantly, armed forces are currently not protecting against foreign threats and actors in cyberspace.

I will first go over the foundations of cyberspace, referring to it not as a 'domain', but as a 'substrate'. Following the definition of PhD Chris C. Demchak at the US Naval War College, cyberspace crosscuts other areas of activity, and is not a single domain[1]. This is followed by the challenges and how they materialise. Finally, the most important part: the defence adaptation to the threats, and what needs to be done.

Cyber as a risk

The fact that cyber is a risk is quite clear, and the evidence is not lacking. In the World Economic Forum's 'The Global Risks Report 2018', they include cyber-attacks as rank number five in the top five list for Europe's greatest risks. However, the threats ranking on two and four, 'Failure of national governance' and 'Failure of financial mechanisms or institutions' respectively, can also be the result of cyber-attacks: the latter being relatively considerable, especially a central threat to privately owned and national banks, and the former because of all sorts of cyber instigated incidents. We need to remember that cyber can be used to achieve power throughout the spectrum of power. Akin to traditional

1 *'[…] For security and military purposes cyberspace is not a domain but a substrate. In our usage, a 'substrate' is an underlying layer on which modern society is built. Cyberspace uniquely underpins all four other war-fighting domains. […] One reason that cyberspace is in fact not strictly a domain is that it is a built environment – imagined, created, developed, sustained, and extended by human intentions and actions.'* Dombrowski, P. and C. C. Demchak (2014). 'Cyber war, cybered conflict, and the maritime domain.' Naval war college review 67(2): 5.

military power, we usually think about a spectrum between hard power and soft power – from which we can command, coerce, threaten and destroy, but also the softer side of power. It is important to remember that adversaries are beginning to understand that they can achieve results by operating with types of power that are not necessarily destructive, not triggering a military response. Thus, I came up with this spectrum:

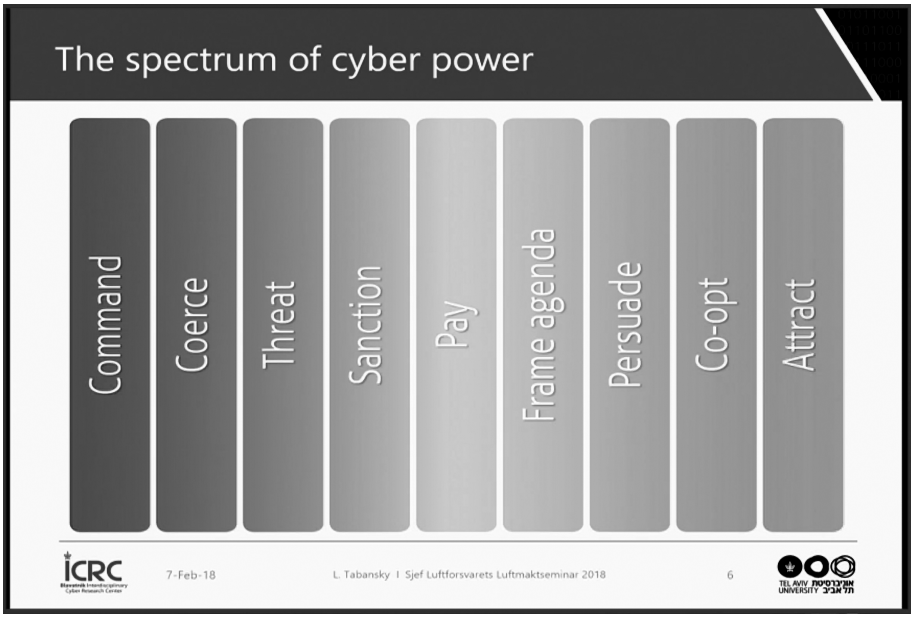


Figure 1: Lior Tabansky's «Spectrum of cyber power».
Source: Presentation on the Air Power Conference 2018, Royal Norwegian Airforce Academy.

Let us go forward with the adversaries, using Russia as an example. Why pick Russia as an adversary, you might ask? I don't simply echo American threat assessments. I use Russia for another reason; Israel (like Norway) now finds itself sharing a common border with Russia through their military bases in Syria, and will continue to do so in the foreseeable future. For the last few years, Russia had not been ranked even amongst the 20 highest threats that Israel has had to consider. Now, the situation changed, and Israel pays much more attention to what Russia's aims and activities are.

So, what does Russia want? It is quite consistent. In summary, everything they see is the West trying to ruin 'Great Russia'. I don't know why, but this is quite clear when talking to Russians. Unfortunately, they only see western conspiracies, operating with a perception of how the West has begun a new model

of warfare. To the general audience in Russia, this western information warfare is written about in a vast number of part-inspirational and part-scientific books and publications. The Russians have identified 24 colour revolutions, beginning in 1989. Among others, the overview goes on to point at China in 1989 and Czechoslovakia in 1993, in addition to more recent ones such as Hong Kong and Ukraine in 2014. Ukraine's Maidan for Russians is a failed western attempt to create a 'Colour Revolution' – a spontaneous, internal revolt overthrowing the existing regime. Furthermore, the so-called 'Arab Spring' and its effects in Syria are viewed as another example of this western type of modern warfare. This is Russia's main threat scenario, and they have been consistent with it. As the regimes fell apart in Egypt and other countries, Dimitri Medvedev, the Russian president said: *'They prepared the same scenario (Arab Spring) for us before, and they will most certainly try it'*[2] – the word 'they' meaning the West, which can be whatever you want it to be, such as the United States and the United Kingdom.

Surprisingly, many relatively well-off Russian middle-class citizens protested in the Russian elections of 2012 against the expected victory of Vladimir Putin. The regime was able to overcome these protests relatively easily. In my view, the regime gained confidence in its threat assessment, because these protests became proof of its accuracy. After a difficult period of confusion, this boost of confidence became a crucial turning point. Importantly, the famous 'Gerasimov Doctrine' must be viewed not as a plan of what the regime wants to do, but as a reflection of their understanding of the world: *'Political goals are now attained through the widespread use of disinformation and other non-military measures deployed in connection with the protest potential of the population'*. Confident enough to publicly publish the doctrine, it does not necessarily outline what they'll do about it, but can rather be understood as a statement signalling that they understand how it works, and therefore they will be able to play according to these new rules of the game.

Hostile Influence Operations (via Social Media)

An example of how Russia operates on the softer side on the spectrum of power *(Frame agenda*, *Persuade*, *Co-opt*, *Attract)* is the 'Lisa Case' in Germany, which NATO declared as the model case of Russia's operations of influence. The model begins with trying to leverage the new media landscape to get information on the targets, followed by targeted messages. Then you create messages

2 Dimitri Medvedev, 22.02.2011: kremlin.ru/events/president/news/10408

to influence public opinion, influencing traditional media to cover the aspects and setting the agenda, including foreign media. This will hopefully lead to political action and the political results that you are trying to achieve.

The Lisa Case was about a girl of Russian origin who went missing in Berlin, which has a large community of Russian expatriates. When the girl didn't return from school, people started looking for her. After some 30 hours, she returned home. In the meantime, the German police had investigated the case of the missing girl and concluded that it was not a kidnapping or something similar, but rather a typical teenage disappearance. However, the Russians were able to spin the case through the media, setting the agenda in Germany and much of the West for over three weeks. Furthermore, especially in Russian media, the disappearance was spun as a story about a Russian girl who had supposedly been kidnapped by migrants, connecting it to German policy for accepting migrants. She was said to have been sexually abused by migrants, and the authorities covered it up because it was not politically correct. In a less than gentle way, the Lisa Case touched the most sensitive issue in German politics at the time.

The operation, which happened on 11th January 2016, was executed in a very beneficial context, as it conjoined with the 2015/2016 New Year's Eve celebrations when supposedly organised mobs had sexually assaulted and raped women, mostly in the German city of Cologne. For some reason, the German media didn't cover the crimes until a couple of days later. This shows that the Lisa Case demonstrates high operational maturity, as the Russians were able to identify fertile grounds and, within days, find a real case and rapidly design an information operation in the right context. Although not very sophisticated, it definitely played out well in the end because they were able to set the political agenda in Germany, in addition to affecting many NATO-countries for three weeks or so. To this day, it is still considered a very successful operation.

Direct attack on homeland infrastructure

One of the main reasons we have defence forces is to prevent adversaries from reaching the homeland. Through cyber, adversaries have the potential to reach and either disrupt or physically destroy homeland targets, without meeting any sort of defences such as border patrols or fighter jets. This has also been demonstrated several times.

An 'experiment' was conducted on Ukraine in December 2015. The Russians succeeded in creating physical results in the sense of blackouts – stopping the delivery of electricity to almost 250,000 customers, purely by cyber means. Interestingly, the areas they targeted were Kiev and a nearby city, both

in the western part of Ukraine. These were relatively sophisticated cyber-attacks, causing not only the disruption of power, but preventing the possibility to remotely restore the power supply. For example, by using the control links to the remote transformer station to re-write firmware on the serial to ethernet converters, they rendered remote control impossible. Clearly, Russian cyber operations can be considered a serious threat.

What can be done?

So, what can we do about it? When talking about traditional warfare, we often speak of reaching political goals. Cyber warfare might be considered to operate below the threshold we are used to. However, it is still warfare, in the sense that it strives to achieve political objectives. An adversary's political objectives may be very different from your objectives. Thus, as we still have a state-based system, in which one state tries to achieve political objectives at the expense of the other, the role for defence forces is to protect the state.

Cybersecurity in Israel

States obviously need to adapt to these requirements. This work has begun in Israel. We have since 2012 the Israel National Cyber Bureau (INCB): a new, non-military civilian organisation charged with developing policies and capabilities, reporting to the Prime Minister. Since 2015, we have the National Cyber Security Authority (NCSA) tasked with carrying out operations to protect the civilian society. The Israeli Defence Force (IDF), however, is not a part of this organisation, rather focussing on protecting itself in order to maintain its necessary capabilities. Thus, we have a parallel effort: one is to protect the entirety of civilian society, including critical infrastructure, and the other is the defence sector and the defence industrial base. In effect, the Israeli state is not solely reliant on its defence sector to protect itself from cyber threats. The system in the US, although too complex to present here, is roughly similar. While US Department of Homeland Security (DHS) is also charged with supporting the efforts of the private sector, but more responsibility rests on the American private sector to safeguard privately owned critical infrastructure against new threats, compared to in Israel. In Israel, Organisations that are designated as critical infrastructure operations receive since 2003 mandatory guidance from the security services on what do to regarding critical IT protection in their organisation. Although it is not the state's responsibility, the state gives organisations some sort of services that cannot be procured on the market, such as new capabilities and intelligence. In summary, regarding

defence services protecting society, we are still way off what we would ideally expect.

Defence adaptation process

Adapting to changing circumstances is not a new situation in warfare. Adversaries have always developed new capabilities, triggering defence adaptation. In security studies, the field of defence adaption is relatively developed – how do organisations innovate and adapt, and more importantly, why don't they do it as quickly or efficiently as you would expect? The process is quite straight--forward.

Phase 1, 'the Serendipitous Invention': the combination of new technologies and new security challenges tends to create a technical and conceptual breakthrough, resulting in a new device or system. When it comes to cyber, we have passed this point several decades ago, evidenced by the discussions in 1970s U.S. defence documents.

In Phase 2, 'Exploitation and Payoff', you ideally start to think about what to do with the systems developed in Phase 1. You need to develop new ideas on how to achieve your goals via system development and deployment. Then, you need to integrate the new devices into a bigger system with changes in doctrine and force structure, which may be less tangible and not as easy to see as the technologies themselves.

Eventually, the ultimate test is to use it in combat; without such a test, it's all a hypothesis, and it's too early to say how to use it properly or whether the innovation is better than what you already had. Regarding cyber warfare, we have fortunately not seen much of its use as a main tool in combat, as opposed to the more common use as a tool of support. However, if we don't increase our ability to defend against cyber-attacks, I think we will find ourselves on the receiving end – clearly not a desired result. Therefore, it is important to start paying more attention to what sorts of defence adaptations are currently being undertaken, and what we can do to improve them.

The West has come far, however. The Joint Strike Fighter programme is the culmination of efforts in the cyber field, such as computer software, sensors, and the fusion of the two. Thus, cyber adaptation is going on in the West, so I'm not stating that the military is ignoring the threat; however, the direction of our adaptation may not be the best path to meet the capabilities that our adversaries are developing.

Conceptualising cyber defence

The new cyber threat is realised by most people, which means that awareness is not the problem, neither are budgets. Meeting the cyber threat is all about decisions, planning, and committing the resources. Conceptually, what can be done?

Perimeter protection

The IT security industry is constantly reminding us how perimeter defence is an inadequate solution – it has always been breached. Unfortunately, we are still doing it. Perimeter defence includes tools such as network segmentation and firewalls. In cyberspace, we do not have borders on the national level. Not because it is technically impossible, but because it brings out the more important political questions about values, and the balance between freedom and human rights vs. security.

Technical innovation (tactical)

A vast amount of technological research and innovations is currently being done, predominantly driven by defence funds in the U.S. and similar countries. However, I don't see these technological innovations, which are available on the market, being integrated into the defence sector. In the IT security market alone, new innovations with an estimated worth of 90 billion USD are made available on the market each year.

Strategic innovation

Ideally, you would come up with a strategic innovation which renders the tools of your adversaries obsolete and irrelevant. However, in the current situation, I'm seeing the opposite. The West do, indeed, have the potential, evidenced by the various defence adaptations being done. But the main threats enabling foreign states to directly reach the homeland targets in our states is still not the focus of these adaptations. This is not a new phenomenon, which in military history is a repeated offence. There is a lot of literature in military history, security studies, and international relations that can be used to assist us in thinking about how to adapt our organisations to meet the cyber threat.

Conclusion

Without successfully adapting, we might find ourselves remaining in the situation that we are currently in – even with the best air, land, and sea forces available, our homelands are still exposed to cyber-attacks. If and when the conflict escalates, we might find ourselves in the situation when the military won't have an enemy to physically fight. The enemy, however, will be able to achieve its objectives and results more quickly, and in a way which confuses our defence and is unpreventable by our military forces.

The current situation is that the possibility of a direct attack is rising. Our defences have become obsolete. What is the use of tanks and aeroplanes if you can only identify an attack after it happened, and on top of that, you can't even identify the attacker? Considering this, we have a lot of work to do. As of today, we currently have no idea what is going on in national networks within countries. We can identify scattered incidents and malware, but we are clueless as to whether these attacks are related to a bigger campaign. Is the malware we find on individual computers unrelated, or is it stepping stones to something different? And it goes without saying that we fail to prevent the malware from reaching its targets in the first place.

Cyberforsvaret – Connecting Commanders

av Inge Kampenes

Fremveksten av et nytt operativt domene, med alt det medfører for en militær organisasjon, er et stort tema – et tema som alle forstår at de bør skjønne, men som de færreste forstår. Jeg skal ikke undergrave min egen autoritet ved å si at *samband* og *digitalisering* er vel så relevante ord som cyber. Så det skal jeg ikke si.

Oppdraget til Cyberforsvaret, om det skal kuttes ned til det absolutt kortest mulige, er Connecting Commanders – vi skal knytte Forsvarets operative sjefer sammen slik at de får drevet kommando og kontroll over styrkene. Og med noen ord ekstra: sikkert samband på moderne krigeres premisser. Sambandet skal være tilgjengelig, og brukerne skal være trygge på at informasjonen kommer frem slik den blir sendt, uten å bli kompromittert. Og moderne krigere kriger i alle domener, også i det nye cyberdomenet, og kapasitetene utvikles etter *deres* behov. Cyber*forsvaret* har ansvaret for å forsvare *Forsvarets* cyberdomene.

Men – tilbake til muligheter og begrensninger i cyberdomenet. Hva er det vi har foran oss? Vi er på god vei inn i en fjerde industriell revolusjon, hvor de teknologiske rammene vil endre seg så radikalt at det får stor betydning for hvordan mennesker og samfunn vil fungere om kort tid. Forhold som automatisert produksjon med roboter, nanoteknologi, elektronisk kommunikasjon og utvikling innenfor bioteknologi, energi og digital økonomi bidrar alle til å endre verdenssamfunnet radikalt. Alle faktorene er drevet av informasjonsteknologi – og digitalisering åpner for nye muligheter som vi ikke engang hadde drømt om for bare få år siden.

Det er ingen hemmelighet at det norske Forsvaret ikke leder denne teknologiske utviklingen. Men det er viktig at vi tar inn over oss endringene og legger til rette for å kunne følge den teknologiske utviklingen som ledes i hovedsak av det sivile næringslivet. Vi er nå i starten av en ny langtidsplanperiode som over de neste fire årene etter min mening vil bli skjellsettende for oss – cybervirksomheten vår må gjennom en omfattende endring for at vi skal kunne tilpasse oss nye behov og forbli en relevant forsvarsaktør.

Femtegenerasjons kampfly har allerede ankommet. Vi må digitalisere resten av Forsvaret slik at vi kan utnytte denne kapasiteten fullt ut. For at vi skal kunne høste full gevinst av et femtegenerasjons kampfly, må også virksomheten rundt flyene, de operative prosessene våre, organisasjonen og kompetansedimensjonen i Forsvaret som helhet tilpasse seg det nye materiellet. Kampflyene markerer et radikalt teknologisk skifte i Forsvaret, og de kommende årene vil vi innføre andre våpensystemer som alle utgjør små teknologiske revolusjoner, som nye ubåter, P-8 overvåkningsfly, kampluftvern, artilleri, luftvarslingsradarer, ubemannede farkoster og satellittkapasiteter. IKT-en i forsvarssektoren og sambandsunderstøttelsen må følge med i denne utviklingen. Vi har store og viktige prosjekter som vi leverer allerede inneværende år, og vi skal investere over fem milliarder kroner de neste fire årene. Disse prosjektene er vi avhengige av å få gjennomført for å levere etterspurte tjenester og opprettholde nødvendig handlingsrom i cyberdomenet.

Samtidig er det også verdt å fremheve at selv om kampplattformene som vi anskaffer, i seg selv er veldig moderne og teknisk avanserte, så betyr ikke det at alle sambandsløsningene som følger med systemene, er like gode. Enten det er logistikksystemer, K2-systemer eller andre – de holder ikke nødvendigvis følge med kvaliteten til kampplattformen som sådan. Og tidvis er også systemene mer ressurskrevende å drifte og vedlikeholde enn det vi strengt tatt skulle ønske. Samtidig må vi erkjenne at på det området er det lite vi får gjort, siden mange av disse løsningene følger med plattformen som en del av pakken. Et eksempel er ALIS (Autonomic Logistics Information System), som skal understøtte F-35 kampfly.

Et annet markant forhold vi står overfor, er renessansen til totalforsvarskonseptet, som nå finner en plass det ikke har hatt siden den kalde krigen. En av grunnene til det er den ubestridelige avhengigheten Forsvaret har til resten av samfunnet dersom vi skal kunne drive effektive militære operasjoner på norsk jord i hele konfliktspekteret. Fremveksten av cyberdomenet bidrar til å viske ut skillet mellom Forsvaret og sivilsamfunnet. I Cyberforsvaret er vi for eksempel avhengige av kraftleverandører og teleselskaper for å kunne løse oppdraget vårt for Forsvaret. Derfor må vi utvikle et godt og vedvarende tett forhold til disse og inngå gode beredskapsavtaler som gir oss nødvendig robusthet og redundans. Og det er i stor grad gjennom cyberdomenet en motstander kan påvirke vårt samfunns kollektive motstandsvilje.

Med dette som tydelige utviklingstrender, hva må vi konkret endre på, for å tilpasse oss fremtiden? Jeg skal ikke gi en utfyllende liste, for den er lang, men jeg vil trekke frem noen av de viktigste forholdene.

Vi må endre på IT-organiseringen i forsvarssektoren, og herunder også

hvordan de forskjellige aktørene samhandler både seg imellom og opp mot eksterne aktører. Vi må også endre på måten vi anskaffer og utvikler IKT-materiell på. Vi må se på innretningen av tjenestene og kapasitetene vi leverer, for antallet enkeltsystemer vi har i dag, utgjør en betydelig sårbarhet, og det er også en vesentlig kostnadsdriver. Ikke minst må vi endre den holdningen som mange av Forsvarets ansatte og ledere har til teknologi, modernisering og digitalisering – og vi må gjøre *mindsettet* vårt mer dynamisk og endringsvillig.

Vi må utvikle et totalforsvarskonsept bygget opp rundt robuste, tilgjengelige og sikre skybaserte tjenester, slik at vi hurtig og sømløst kan utveksle informasjon med utvalgte aktører uten tap av tid og uten å risikere operasjonssikkerheten vår.

For at Cyberforsvaret skal forbli relevant for Forsvaret i en slik kontekst, er det avgjørende at vi utvikler tett og god samhandling med andre lands cyberforsvar, med forskningsmiljøer og akademia, med sivil industri og bedrifter og med organisasjoner i andre statlige sektorer med tilsvarende utfordringer som de vi står overfor. Slikt samarbeid setter oss i stand til å forstå felles utfordringer og hvordan de kan løses, og det bidrar til nødvendig kvalitetsheving av våre leveranser. En slik kvalitetsheving medfører at andre ønsker å samarbeide med oss, og det tiltrekker seg ny og nødvendig kompetanse. Samarbeid gir kvalitetsheving gir kompetanse gir mer samarbeid og mer kvalitetsheving – kort oppsummert: en god sirkel.

Kompetanse er et nøkkelord innenfor vår virksomhet. Vi forstår nok ikke i tilstrekkelig grad det nye domenet ennå. Jeg tror ikke det norske Forsvaret er i en særstilling her; mange av våre allierte famler også rundt og forsøker å finne ut hvordan de militært skal tilnærme seg utfordringene og mulighetene som følger med cyberdomenet. Men vi har et godt utgangspunkt. Det norske samfunnet er blant de mest digitaliserte i verden – og det betyr at de som kommer inn i Forsvaret i dag, har et godt fundament av teknologisk forståelse og en evne til å se potensialet i teknologi – i mye større grad enn min generasjon.

Jeg tror utdanningsreformen gir oss spennende muligheter. Vi får en dedikert cyberingeniørskole i Forsvaret, bygget videre på grunnmuren Forsvarets ingeniørhøgskole. Det vil forhåpentligvis også føre til at cyberdomenet og forståelse for cyberdomenet kommer inn på pensum i alle Forsvarets utdanningsløp. Det vil gi oss et fortrinn fremfor mange andre nasjoner, men også gi oss et bedre grunnlag for å forstå domenet og dets muligheter og utfordringer med hensyn til militære operasjoner. Det vil dessuten forenkle implementeringen av de beslutningene og retningsgivende dokumentene som må følge med det nye domenet.

Innføringen av spesialistkorpset tror jeg også vil hjelpe oss betydelig på

veien. Dersom vi lykkes med å få på plass en stabil kompetansebastion som støtter sjefene våre – gjerne med lengre ståtid i stilling –, vil deres styrkede kunnskap og forståelse være til betydelig støtte for virksomheten som helhet. Dette gjelder ikke minst i møte med de komplekse sammenhengene og mulighetene som ligger i grensesnittet med andre avdelinger, grener og kapasiteter.

Hvordan jobber vi så med forebyggende sikkerhet og cybersikkerhet for å kunne opprettholde nødvendig handlingsfrihet i cyberdomenet? Cyberdomenet bærer i seg nærmest uendelig kompleksitet, og alt henger sammen med alt. Så også sikkerhetsutfordringene. Når vi snakker om cybersikkerhet, så har det mange sider ved seg. Når vi skal opprettholde cybersikkerhet i Forsvaret, for å se på det som en sluttilstand, er det flere forhold som må ligge til grunn.

Om vi ser for oss en pyramide, vil grunnplanet i pyramiden være systemdesign og systemarkitektur. Vi må tenke sikkerhet allerede når vi kjøper eller lager systemene våre, slik at vi etablerer løsninger som er sikre nok, og som kan forsvares. Det er en betydelig jobb, og her har Forsvaret mye materiellarv som dessverre rett og slett ikke er god nok.

I løpet av de neste månedene vil vi innføre et felles sikkert og beskyttet ugradert nett i Forsvaret. En av våre største sikkerhetsutfordringer har vært det enorme antallet ugraderte systemer som er koblet til nettet, og som ikke er designet med sikkerhet som forutsetning. De systemene vil vi til livs, og hovedinnføringen vil skje i forkant av den store NATO-øvelsen Trident Juncture nå i høst. Dette reduserer sårbarheten i systemene våre og hever terskelen for angrep gjennom ugraderte løsninger.

Kryptografi er en viktig ramme i planlegging og tegning av en sikker systemarkitektur. Norge var i sin tid verdensledende innenfor krypto – det kan vi ikke si at vi er i dag. Det er en bekymring – spesielt siden det kommer teknologi på markedet de neste årene som gjør det atskillig enklere å knekke kryptoalgoritmer. I lys av både Forsvarets og samfunnets tydelige avhengighet av digitalisering i dag og i fremtiden er nettopp kryptografi et område som det er vel verdt å investere ressurser i.

Når grunnplanet i cybersikkerhetspyramiden er etablert, er det viktig å erkjenne at et system som er sikret i dag, ikke vil være sikkert for all fremtid. Trusselaktørene utvikler seg, nye sårbarheter blir funnet, og en angrepsvektor som er umulig i dag, kan være offentlig kjent i morgen. Det har vi sett flere eksempler på i løpet av det siste året, og det har også vært rapportert flere hendelser i mediene og den offentlige debatten. Det er derfor viktig å revurdere systemene kontinuerlig og søke etter sårbarheter som må rettes opp og utbedres. Det er et nærmest uendelig arbeid – og det er møysommelig og tidkrevende arbeid. Samtidig er det svært viktig, spesielt for dem av oss som står over-

for høykompetente trusselaktører som fortløpende videreutvikler kapasitetene og kapabilitetene sine.

Når systemene er etablert og sikret, er vårt viktigste førstelinjeforsvar den årvåkenheten og sikkerhetskulturen som brukerne av systemene representerer. Motstanderne våre benytter seg ofte av enkleste vei inn i IT-systemer, og den veien er vedlegg til elektronisk post, eller lenker i e-post. Det høres kanskje banalt ut – men dersom en motstander først får tilgang til systemet gjennom elektronisk post, så kan veien inn i resten av de graderte datasystemene være kort og rimelig enkel.

Over den enkelte bruker ligger organisasjonens sikkerhetstiltak og rammer. Disse omfatter alt fra organisatoriske til mer fysiske tiltak. Adgangskontroll spiller en rolle, siden det hindrer fysisk tilgang til maskiner. Kurs og utdanning, rollen til lokal sikkerhetsoffiser og datasikkerhetsleder – alt dette bidrar til å skrelle av og redusere trusler. Datasikkerhetslederne rundt om i Forsvarets avdelinger og garnisoner burde, for øvrig, ha større autoritet og myndighet enn de har i dag – de gjør en svært viktig jobb.

Mot toppen av pyramiden kommer de som vi ofte tenker på når vi snakker om cybersikkerhet: miljøene som driver deteksjon og analyse på systemene våre. Men det er viktig å erkjenne at om det ikke hadde vært for alle de andre trinnene i pyramiden, så hadde jobben deres vært helt umulig – til dels fordi antallet inntrengninger hadde vært så enormt at det hadde vært umulig å håndtere dem, men også fordi de hadde måttet bruke tid og energi på så mange bagateller at de ikke hadde fått mulighet til å fokusere på de viktigste truslene.

Helt på toppen av cybersikkerhetspyramiden vår finner vi militære defensive cyberoperasjoner. Her snakker vi om taktikk, doktrine og operative tiltak for å sikre handlefrihet i cyberdomenet og at motstandere ikke evner å forstyrre operasjonene våre, og tiltak for å øke vår operative evne. Dette er veldig gode tiltak, men det er også handlinger som ikke betyr særlig mye med mindre hele resten av cybersikkerhetspyramiden er etablert og den er robust og fungerer som planlagt.

Det er viktig å fremheve at cybersikkerhetsarbeidet ikke utføres for vår skyld, og definitivt ikke for IT-systemenes skyld. Det er noe vi prioriterer for Forsvarets skyld og av hensyn til operasjonene våre. Med tanke på hvor avhengige vi er av sambandssystemene våre, er cybersikkerhet i bunn og grunn operasjonssikkerhet.

Så vil jeg vie oppmerksomheten til cyberoperasjoner og hvordan cyberdomenet skal forstås i en slik kontekst.

Vårt fagområde, cybersikkerhet og samband, er altså i utvikling, til dels som følge av teknologien, men også som følge av at den militære tenkingen

rundt teknologi er i endring. NATO anerkjente cyberdomenet som et operativt domene sommeren 2016. Alliansen jobber nå med å få på plass en operativ doktrine for cyberoperasjoner. I denne vil tenkingen dreie seg om å trekke cyberoperasjoner inn i allierte fellesoperasjoner, og den planlegges og operasjonaliseres som alle andre operasjonsfunksjoner.

AJP-3.20 vil være en doktrine i operasjonsserien, 3-serien, og det vil være én doktrine for cyberoperasjoner. NATO river med det ned skillet mellom offensive og defensive operasjoner i cyberdomenet og søker, slik jeg leser det, å gjøre cyberoperasjoner til et mer «stuerent» operasjonskonsept. De vil søke å trekke cyberoperasjoner ut av skyggene og inn i de ordinære og løpende planprosessene for militære operasjoner.

Det har mange fordeler. Rent operativt blir det selvsagt enklere å forholde seg til, siden en tydeligere operativ prosess gir et klarere og tydeligere plangrunnlag og en mer sammenhengende operasjonsplanlegging. Folkerettslig og konvensjonsmessig blir det enklere å forholde seg til cyberoperasjoner på lik linje med andre operasjoner. Og – kanskje viktigst for meg – det blir enklere å se de tette båndene som eksisterer mellom cyberoperasjoner, samband og cyberdomenet.

Cyberdomenet har mange interessante muligheter som vi bare så vidt har begynt å utforske. I motsetning til landjorda, lufta og sjøen er cyberdomenet skapt av mennesker. Det eksisterer ikke av seg selv. Vi etablerer det – bygger det ved å etablere samband, knytte sammen IT-nettverk og knytte sammen systemer og plattformer. Ved å etablere nettverkene og koblingene skaper vi vårt eget domene, som vi er avhengige av for å muliggjøre operasjonene våre.

Vi utvider og tilpasser domenet til våre operative behov slik at domenet er der når man trenger det, i tid og rom, og på den måten ivaretas den operative sjefens behov. Når vi skal forsvare vår del av domenet, kan vi også forme det i defensiv hensikt. Vi kan styrke det der hvor den operative sjefen har sitt tyngdepunkt, og svekke det der hvor vi ønsker at en motstander skal ha sitt fokus. Vi kan også fjerne deler av kartet når det ikke er nødvendig, for å redusere vår risiko, og vi kan flytte og endre på lendet for å frustrere eller forvirre en motstander. Mulighetene er betydelige.

I Forsvaret er Etterretningstjenesten fagmyndighet for cyberoperasjoner, og Cyberforsvaret har ansvar for defensive cyberoperasjoner. Vi må i fremtiden sammen evne å utnytte de mulighetene som cyberdomenet gir, for best mulig å understøtte sjef Es, sjef FOHs og de taktiske styrkesjefenes operasjoner.

Jeg tror cyberoperasjoner utvikler seg mot å omfatte tre hovedoppgaver: «Defend the Network» (forsvare nettverket), «Define and Exploit the Attacker» (finne og gå til kamp mot angriperen) og «Shape the Battlefield» (forme

slagmarken). Hovedoppgavene må håndteres både hver for seg og sammen. Her er det oppgaver nok for Cyberforsvaret, E-tjenesten og FOH.

Mot slutten av foredraget vil jeg komme med noen påstander om hvordan cybervirksomheten i forsvarssektoren bør utvikle seg innenfor den nåværende langtidsperioden, altså frem mot 2021. Vi bør utvikle oss mot å bli en virksomhet som har et tydeligere operativt fokus og er anerkjent som en støttespiller for militære operasjoner – på moderne krigeres premisser. Vi må være en integrert del av Forsvarets operative virksomhet slik at vi best mulig kan understøtte dere – både operativt og på forvaltningssiden. Og vi må fungere som én koordinert virksomhet som evner å stå sammen, med felles prioriteringer og med oppmerksomhet på felles løsninger – slik at vi best mulig kan løse våre oppdrag.

Forsvaret trenger en cybervirksomhet som evner å hurtig omsette mulighetene som teknologien gir til å realisere et høyteknologisk forsvar med maksimal operativ evne, og som samtidig evner å gjøre det på en ressurseffektiv måte slik at størst mulig andel av budsjettene våre kan gå til soldater, våpen, fly, fartøy, kjøretøy og etterretningskapasiteter. Og vi bør være ledende innenfor cybersikkerhet i Norge og dermed også et forbilde for andre aktører i samfunnet. Særlig er dette viktig i lys av at Forsvaret sitter i en unik posisjon og har et unikt innblikk både i trusselbildet, i trusselaktørenes kapasiteter og i mulige konsekvenser ikke bare for Norges militære evne, men også for samfunnet som helhet.

Vi i Cyberforsvaret skal ikke ta på oss ansvaret for cybersikkerheten til hele Norge; det vil vi aldri ha kapasitet eller ressurser til. Men jeg tror vi må innta en mer aktiv rolle i å styrke samfunnets bevissthet, forståelse, kunnskap og kompetanse innenfor området. Det vil tjene våre interesser siden vi er avhengige av at sentrale samfunnsfunksjoner fungerer som normalt når vi skal løse våre oppdrag.

Trusselbildet er sammensatt og komplekst, og det er mange aktører som opererer her, men det er viktig å erkjenne at cybertrusselen er grenseoverskridende og sektorovergripende. Norge har etter min vurdering ikke tilstrekkelige mekanismer på plass til å beskytte seg i møte med disse utfordringene. Det er flere politiske prosesser i bevegelse for å håndtere dette gapet, men dessverre ligger nok de fleste av dem noe frem i tid.

Jeg har delt noen refleksjoner med dere om hvor Cyberforsvaret står med tanke på cybervirksomhet, cyberoperasjoner og cyberdomenet – og hvordan vi bør utvikle oss. Jeg har snakket om hva som er mulighetene våre, og også om noen av utfordringene som følger med det å utnytte cyberdomenet til militære formål.

Vi står overfor store endringer, og utfordringer som følger med disse, men Forsvaret har også store muligheter når vi nå får ressurser til modernisering og digitalisering. Med det investeringsgrunnlaget som er planlagt for inneværende langtidsperiode, så har jeg tro på at vi skal få det til.

Det nye domenet fører med seg omfattende kompetanse- og sikkerhetsutfordringer, men samtidig har vi kapasiteter på plass som ser på cybersikkerhet i et sammensatt og operasjonsfokusert perspektiv. Med arbeidet som pågår i NATO-alliansen, håper vi at mye av det doktrinelle og konseptuelle grunnlaget for cyberoperasjoner vil være på plass i nær fremtid. Dette vil gi oss et bedre fundament å bygge forståelse og fremtidige operasjoner på. Det fundamentet vil være nødvendig når vi tar inn cyberdomenet og cyberoperasjoner i Forsvarets fellesoperative doktrine, det vil si når den revideres og utgis i en oppdatert versjon senere i år.

Fem råd for en bedre debatt

av Harald Høiback

Jeg jobber fremdeles ved Forsvarets stabsskole, eller rettere sagt på skolen som tidligere var kjent som Forsvarets stabsskole. Den skifter navn stadig, men akkurat nå tror jeg den heter Institutt for militær frustrasjon og endringsangst. Som dere skjønner, er det ikke vi selv som bestemmer navnet – vi militærakademikere bestemmer ingenting. Makten sitter hos dem som kontrollerer Excel-arket. Forrige gang jeg holdt et innlegg her, sa jeg at jeg ikke hadde noen ambisjoner om å teste takhøyden på Luftkrigsskolen. Men jeg oppdaget raskt at heller ikke Luftkrigsskolens auditorium har himmelen selv til tak. Det ble derfor strekk og formaninger da jeg kom hjem, da jeg kom i skade for å si noe ufordelaktig om utdanningsreformen. Nå, derimot, har jeg latt meg fortelle at det er *så* 2017 å være negativ til utdanningsreformen. Nå er vi alle for. Spørsmålet nå er selvfølgelig hva jeg kan stille meg negativ til som det i fremtiden vil oppfattes som *så* 2018 å være skeptisk til. Hva passer da bedre enn å være skeptisk til vår evne til nettopp å spå fremtiden? Når vi diskuterer fremtiden og fremtidig utvikling av Luftforsvaret, herunder Multi-Domain Battle, er det selvfølgelig ytterst viktig at vi makter å slippe tankene fri.

Etter mitt syn er det tre filosofiske hovedutfordringer knyttet til militær fremtidstenkning og utvikling. Punkt 1: Hvordan skal vi sikre at alle gode ideer faktisk kommer på bordet? Eller sagt på en annen måte: Hvordan kan vi best mulig sikre oss mot ubehagelige overraskelser i fremtiden? Punkt 2: Hvordan makter vi i fredstid å luke bort alle «gode ideer» som kanskje ikke er så gode likevel, når det kommer til stykket? Hvordan klarer vi å unngå å kjøre såpass langt ned en blindgate at vi aldri rekker ut før det er for sent, eller før vi har brukt uhorvelige milliarder av skattebetalernes penger? Punkt 3: Det hjelper ikke at noen her på haugen, eller andre hauger for den saks skyld, har sett lyset, om de ikke er i stand til å formidle den innsikten til dem som sitter med pengesekken og beslutningsmakten.

Jeg skal ikke snakke om svarte svaner, «black swans», som man gjerne gjør på seminarer som handler om fremtidige trusler. Jeg tror nemlig at frykten for svarte svaner er sterkt overdrevet. Vi som bor inntil Østmarka, er skeptisk til ulv, men ikke til svarte svaner. De har aldri tatt sau, bikkjer og langt mindre folk.

Uavhengig av om vi snakker om teknologisk utvikling i fremtiden eller om utviklingen av menneskelige ressurser i Forsvaret, bør vi altså legge forholdene så godt til rette vi bare makter for fri flyt av tanker og ideer. Resten av dette innlegget vil jeg bruke til å gi fem tips og spilleregler for hvordan debatt og meningsutveksling bør foregå om vi ønsker å lykkes med de tre hovedutfordringene. Ikke overraskende vil jeg avslutte med å hevde at vi ikke er spesielt gode på dette heller. Det er derfor jeg blir invitert til dette establishmentet – for å dempe entusiasmen. Blir man for livsbejaende her oppe, får vi i Oslo-gryta gjerne en telefon.

De fem tipsene jeg har kommet frem til for å sørge for god idémyldring, er følgende:

1 Sjefer og myndighetspersoner må ikke plante flagg (Mandelas lov).
2 Ta aldri mannen, *kun* ballen.
3 Trekk aldri forskerkortet.
4 Når det gjelder fremtiden, *vet* vi ingenting!
5 Hva *du mener*, spiller ingen rolle!

1 Når alle vet hvor sjefen står

Sjefer kan oppfordre til åpenhjertig debatt så mye de vil. Men i det øyeblikket de selv hiver seg med i debatten, lukkes lukene. Om sjefene ønsker fri flyt av tanker og ideer, må de derfor ikke markere egne standpunkter. Sjefen må sørge for gode rammer for debatten, men ikke innholdet i den. Dette er Nelson Mandelas ledertips nummer én. Det han hadde lært av sin far, landsbyhøvdingen, var at høvdingen alltid tok ordet helt til slutt i møter.

Det krever imidlertid et moralsk mot. Samtalen kan nemlig ta andre veier enn sjefen ønsker. Ønsker sjefen derimot å ta livet av en debatt, er det å plante eget flagg i terrenget det mest effektive han kan gjøre. Når folk med makt over folks fremtidsutsikter markerer standpunkt, skrur de av debatten. Da er det bare påfugler og dødsdømte igjen. Problemet med å skru av debatten er selvfølgelig at problemet som debatteres, ikke forsvinner av den grunn. Jeg anbefaler derfor alle å lese boken til Svetlana Aleksijevitsj, *Krigen har intet kvinnelig ansikt*:

> Før krigen gikk det rykter om at Hitler gjorde seg klar til å angripe Sovjetunionen, men slike samtaler ble det brått satt en stopper for. De ble stoppet av dertil egnede organer. Du vet hva slags organer – NKVD, Tsjekistene. Hvis folk hvisket til hverandre, så var det bare hjemme på kjøkkenet og i kollektivleiligheter.

> Bare på sitt rom, bak lukkede dører eller på badet etter å ha åpnet vannkranen. (Aleksijevitsj, *Krigen har intet kvinnelig ansikt*.)

Poenget, mine damer og herrer, er at vanskelige spørsmål ikke blir borte selv om vi bestemmer at vi ikke vil snakke om dem. Russernes problem ble langt større fordi de nektet å se realitetene i øynene. I vår bransje kan konsekvensene av kollektiv taushet bli verre enn ubehagelige oppslag i VG.

Det var det første punktet. Sjefer og ledere, hold dere unna om dere ønsker en åpenhjertig og fri debatt. Dere har makt til om ikke å skru av debatten, så i det minste å fortrenge den til messer, korridorer og lukkede Facebook-grupper. Men problemet forsvinner ikke av den grunn, selv om det kan kjennes behagelig en stund. Sørg heller for en god debattarena og et godt debattklima. Og er det slik i dagens Norge at man kun kan diskutere viktige ting gjennom overskrifter, bør det være sjefers fremste rolle å bekjempe den tendensen, ikke å forsterke den. Om sjefer og ledere kommer i skade for å få i seg for mye Møllers tran en dag, er det derfor bedre å ta seg en tur i trimstudioet eller svømmehallen enn å gå løs på forvirrede meningsmotstandere langt nede i hierarkiet. Dette leder meg til neste punkt.

2 Ta ballen!

Det andre punktet gjelder debattanter av alle slag, og ikke bare sjefer og andre utvalgte. Om målet er fri flyt av meninger med den hensikt å øke kompetansen og gjøre oss best mulig forberedt til fremtiden, er det viktig at man tar ballen og ikke mannen. Man bør heller ikke ta stråmannen.

Bruk av stråmenn er å tillegge motstandere en oppfatning de ikke har, men som det er mye lettere å kritisere enn oppfatningen de egentlig har. Piet Hein ga følgende fengende beskrivelse av fenomenet: «En yndet form for polemikk består i det probate trick, at dytte folk en mening på hvis vanvidd alle kan forstå.» I en fruktbar debatt er det imidlertid argumentene og saksfremleggene som er relevant, ikke hvem som kommer med dem. Om du har forsket på temaet herifra til månen, spiller ingen rolle. Det er det mange som sliter med å forstå. Det er ingenting i veien for at en tomsing uten et gram studiepoeng kan komme opp med et godt argument eller en relevant saksopplysning. Sagt på en annen måte, hjelper det ikke om du er en god sjakkspiller, om du spiller dårlig.

Nå er det selvfølgelig slik at gode sjakkspillere har en tendens til å spille bedre enn de svakere. Det er derfor vi oppfatter dem som gode. Men også de kan gjøre dårlige trekk, og trekket blir ikke bedre av at det er en stormester som gjør det.

Når du går etter mannen, gjør du det fordi du ikke ønsker å ha motstanderen i arenaen. Å ta personen istedenfor argumentet er imidlertid ganske uheldig om man ønsker å få gode ideer på bordet.

Oppfinnelsen av aksjeselskap er en av de viktigste forutsetningene for den velstands- og rikdomsveksten vi har sett i vår del av verden siden 1800-tallet. Det geniale med aksjeselskap er det såkalte begrensede ansvar. Om selskapet går konkurs, vil ikke eierne miste mer enn det de har investert i selskapet. De mister ikke alt de eier. Det gjør at de tør å investere i risikoprosjekter som kan gi stor avkastning, men som også kan gå over ende. Om man ønsker en fruktbar militærfaglig debatt om fremtiden, må det også være slik når man utveksler ideer, ikke bare ved utveksling av aksjeposter. Som Nils Arne Eggen sier: «Det spiller ingen rolle hvem som kommer med de gode ideene, bare de kommer.» Debattdeltagerne bør imidlertid ikke fordre for mer enn sine argumenter, ikke hele sin troverdighet.

Om man kommer opp med en idé som ikke viser seg å holde i møte med virkeligheten, bør man kunne likvidere ideen uten at man også likviderer avsenderen. Det kan jo hende at vedkommende har mange andre innsikter og ideer enn denne ene dårlige. Men hvem tør sende spenstige ideer ut på markedet om man risikerer å bli slått personlig konkurs, i form av at man blir fratatt alt av fremtidig troverdighet om det viser seg at tankene ikke holdt vann?

Winston Churchill hadde mange gode ideer, og enda flere dårlige. Til tross for det sa han: «No idea is so outlandish that it should not be considered.» Hvis vi skal komme frem til gode ideer i fremtiden, må vi også tenke slik. Ingen ideer er for dumme til å luftes. Mange ideer er for dumme til at de bør iverksettes. Men om vi ikke tør å fremme synspunkter som vi ikke er helt sikre på at alle viktige personer deler, står vi i fare for å knekke verre ting enn ankelen.

Dette var altså den andre regelen – man *er* ikke sine standpunkter. Man har et standpunkt til man av ulike grunner inntar et annet. Det er et ytterst prisverdig element ved oss mennesker at enkelte eksemplarer av arten er i stand til å endre standpunkt som følge av ny kunnskap. Det skjer bare om noen tør å sende uvanlige argumenter inn på markedsplassen, uten frykt for varige men.

3 Trekk aldri forskerkortet

Det tredje tipset for åpen debatt går ut på at man i en debatt aldri skal trekke forskerkortet. Det høres kanskje merkelig ut og krever en forklaring. Dette er i tråd med det jeg nettopp nevnte: Man *er* ikke sine standpunkter. Det er selvfølgelig grunn til å anta at en som har forsket eller har bred erfaring på andre

måter, har bedre forutsetninger for å komme frem til gode argumenter enn folk som ikke har den bakgrunnen. Men dette er det ingen automatikk i. Det er ikke slik at alle kroppslyder fra biskopen er teologi. Det er heller ikke slik at alt det fagfellevurderte akademikere eller høyt dekorerte intopsere lirer av seg, er spesielt lurt. Det er argumentene som bestemmer om argumentet er godt, ikke avsenderen.

Hvis kravet til å delta i en debatt er at du har doktorgrad i ett eller annet, blir det mye akademisk innavl og ryggklapping. Om det er slik at vi ikke kan skille gode argumenter fra dårlige argumenter på annen måte enn om vedkommende har et vitnemål fra ett eller annet fakultet, står faget ganske svakt. Hvis det eneste argumentet du sitter igjen med, er at «dette har jeg da studert», er det bedre å studere litt til enn å så tvil om andres rett til sine synspunkter. Det er tilsvarende i idretten. Man antar at de som har trent mest og best vinner gullmedaljene. Men det er ikke slik at den som kan vise frem den mest imponerende treningsdagboken, vinner. Ikke i det hele tatt. Det er prestasjonene den dagen som avgjør resultatet.

4 Om fremtiden vet vi ingenting!

Det fjerde punktet er ganske enkelt. Når vi snakker om fremtiden og fremtidig utvikling, vet vi ingenting. Når folk kvitterer ut en hendelse ved å si at «det har jeg visst hele tiden», tar de feil. Man kan kun ha kunnskap om fakta, og det ligger ingen kjente fakta i fremtiden. Det finnes kun gode eller dårlige grunner for å anta dette eller hint om fremtiden. Disse grunnene har best vekstvilkår om man holder seg med en stor takhøyde for å lufte tanker om fremtiden. Og til dere kadetter: Dette må ikke misforstås. Det er fullt mulig å vite en hel masse, også på eksamen. Men om fremtiden vet vi ingenting. Det er derfor viktig at dere dyrker evnen til å tenke vidt og bredt. Etter at dere har fylt 40, er det for sent.

5 Hva du mener, spiller ingen rolle!

Det siste punktet går selvfølgelig på dette «likes-okratiet» som brer om seg. Ganske mange synes å være av den oppfatning at fyrop, heiarop og tomler opp eller ned på en eller annen måte bidrar til sakens opplysning. Jeg er innforstått med at likes kan ha en misjon når man diskuterer kakeoppskrifter eller fotballag. Men jeg stusser over at det også oppfattes som fruktbart i diskusjoner om Forsvarets fremtid og videre utvikling. Min bekymring er at militær meningsutveksling koker ned til dette, og kun dette. Da er jeg redd fremtidens overras-

kelser blir av den ubehagelige sorten. Det kan, mine damer og herrer, komme en dag hvor det dukker opp problemer som ikke kan løses med et smilefjes. Noen problemer krever pistol.

Avslutning

Nå har jeg vært gjennom alle fem lover man må følge om man ønsker idémyldring og teoritesting andre steder enn på havets bunn:

1 Sjefer og myndighetspersoner må ikke plante flagg om vi ønsker en åpen debatt.
2 Man må aldri ta mannen, *kun* ballen, med mindre det er mannen man ønsker å ta.
3 Trekk aldri forskerkortet eller antallet deployeringer-kortet, med mindre du ønsker å signalisere at du begynner å gå tom for saklige argumenter.
4 Når det gjelder fremtiden, *vet* vi ingenting!
5 Hva *du mener*, spiller ingen rolle for kunnskapsveksten. Kun de argumentene du eventuelt er i stand til å fremme.

Noen vil selvfølgelig si at jeg nå ikke har gjort annet enn å slå inn åpne dører, og at Luftkrigsskolen burde ha brukt pengene sine bedre enn å kjøpe flybillett til meg. Ingen er spesielt uenige i dette. Eller rettere sagt: Mange er sikkert både enige og uenige, men jeg kan ikke se for meg at det finnes så mange saklige argumenter mot disse fem, annet enn å stille spørsmål ved hvor mange døgn jeg har i knappetelt.

Så hvorfor bruke min tilmålte tid til å minne forsamlingen om selvfølgeligheter? Poenget, selvfølgelig, er at det selvfølgelige ikke er så selvfølgelig som vi liker å tro. Spesielt ikke når det står viktige ting på spill. Den nobelprisvinnende psykologen Daniel Kahneman sier følgende om livets selvfølgeligheter:

> Uheldigvis er det når denne fornuftige fremgangsmåten trengs som mest, at det er minst sannsynlig at den vil bli benyttet. Vi skulle gjerne hatt en varselklokke som ringer høyt når vi er i ferd med å gjøre en stor feil, men det finnes ingen slik klokke, og kognitive illusjoner er generelt vanskeligere å gjenkjenne enn sansebedrag. Fornuftens stemme er gjerne mye svakere enn den høye og klare stemmen til en feilaktig intuisjon, og det er ubekvemt å tvile på intuisjonen når du er stresset på grunn av en viktig beslutning. Mer tvil er det siste du ønsker deg når du har problemer: Resultatet er at det er mye lettere å påvise et minefelt når du ser andre vandre ut i det enn når du selv gjør det. Observatører har det mindre

travelt kognitivt enn aktører og er mer åpne for informasjon. (Daniel Kahneman, *Tenke, fort og langsomt*)

Så når det drar på seg, viser det seg altså svært vanskelig å holde seg til de fem punktene som jeg har presentert her. Vi kan ty til et nærstående eksempel, og hold dere fast. Besto oberstløytnant Harald Høiback VG-testen i saken «Oberstløytnant: – For mange kvinner i Forsvaret svekker Norges stridsevne»? Neppe. Men istedenfor å slå mannens argumenter i hjel med bedre argumenter brøt man etter mitt syn fire av de fem kravene vi har gått gjennom her.

Flaggoffiserer og statsråder snublet i benene på hverandre, ikke for å angripe argumentene, men for å angripe han som argumenterte. Her skulle det knekkes ankler på en måte som gjorde at ingen andre ville våge seg ut med slike dumheter igjen. Mannen hadde åpenbart heller ikke forsket nok, eller sovet nok i telt. De fleste som kastet seg inn i debatten, hadde heller ingen motargumenter og fant det heller ikke nødvendig. Å signalisere hva man mente om saken og om oberstløytnant Høiback, ble det sentrale.

Problemet her er selvfølgelig ikke om det er for mange eller for få kvinner i Forsvaret. Temaet er vår evne til å diskutere vanskelige ting. Om alt som er vondt og vanskelig, feies under teppet, vil vi på ett eller annet tidspunkt gå på trynet. Også ved «Air Power in Future Joint Operations» blir det ganske lite å glede seg til om kortsiktige bekvemmelighetssyn skal få bestemme takhøyden i debatten.

Men vi er ikke her for å diskutere ubehagelige ting. Vi er her for å hygge oss og møte gamle kjente over en halvliter eller ti. Dette var egentlig det sjette rådet for en åpenhjertig debatt – ikke inviter kranglete og hevngjerrige akademikere til å holde epilog. Det blir bare dårlig stemning av det, og ikke får dere replikk heller. Dere kommer ikke engang til å huske mine fem råd for en god og åpen idémyldring. Det de fleste av dere kommer til å sitte igjen med, er at svarte svaner ikke er noe å frykte.

FOHs syn på Multi Domain Battle

av Lars Christian Aamodt

All honnør til Luftforsvaret og til LKSK for nok en gang å ha valgt et interessant og tidsriktig tema. Dere evner å se inn i glasskula og starte gode diskusjoner som en forutsetning for å finne tidsriktige og gode løsninger, tilpasset oss og våre behov som nasjon og som alliert. Initiativet svarer også godt på General David D. Perkins, US Army Commanding General, sin etterlysning i forordet til Multi Domain Battle (MDB)-publikasjonen: Evolution of Combined Arms for the 21st Century, hvor han skriver: «et helhetlig, multi-service, inter-organisatorisk og **multinasjonalt engasjement og involvering mangler.**» Kanskje det er en av grunnene til at versjon 2.0 av publikasjonen allerede er i prosess.

MDB starter med et koordinert initiativ og en koordinert tilnærming mellom US Army og US Marine Corps. Arven ligger i Air Land Battle-doktrinen. Hensikten er på ny å forsøke å nedkjempe en såkalt «near peer adversary» ved en smartere og mer helhetlig tilnærming, inklusive integrert anvendelse og utnyttelse av domener av nyere dato. Hovedforskjellen er en forståelse av at operasjonsområdet ikke lengere er fysisk delt inn i deep, close & rear, at de operative problemstillingene kan angripes systematisk langs en skjematisk linje og at ulike virkemidler er tilpasset de enkelte stridsområdene. Det fremtidige stridsfeltet er mer komprimert, ønsket effekt kan oppnås med andre virkemidler, avhengighetene for å lykkes har andre sårbarheter, tempo og våpenrekkevidde har økt, presisjonsvåpen, fiberkabler og satelittsystemer gjør nær sagt alle mål, fra baser, våpensystemer, logistikk kjeder, ja sågar ned på enkeltindivider, sårbare og tilgjengelige, hele tiden.

Det at US Marine Corps (USMC) er en del av motoren i MDB-utviklingen betyr mye for oss, rett og slett fordi USMC definitivt er en forventet tung støttespiller med en tung plass i vårt nasjonale planverk, og som vi derfor må fungere godt sammen med i krise, konflikt & krig, sågar også i daglige trening, øving og annen aktivitet. Går USMC den veien, så må nok vi bevege oss i samme retning. Spørsmålet er dermed ikke om MDB kommer til oss, men som Sj Luft kommenterte på Facebook i oppkjøringen til dette seminaret, det er et spørsmål om når.

Fra det operasjonelle ledernivået i Forsvaret er det umiddelbart flere reflek-

sjoner som gjøres når US-ledede MDB som konsept og stridside presenteres og diskuteres:

Det søkes å utvide domenekunnskap og operativ domeneforståelse og nye operative muligheter ved å fullt ut integrere space, cyberspace og også det elektroniske krigføringsdomene i konseptet, ikke bare som domener som benyttes for å understøtte operasjoner i de tradisjonelle land-, sjø- og luftdomenene, men som domener hvor strid i en annen form kan utkjempes, og hvor kamper kan vinnes og eller tapes uten tradisjonell kinetisk strid, manøver og våpenutveksling. En erkjennelse av denne domenetilnærmingen øker kompleksiteten, skaper nye muligheter, utfordrer ytterligere situasjonsforståelse og stiller nye og skjerpede krav til oversikt, kunnskap og ledelse eller kommando og kontroll (K2) om du vil, kanskje særlig på det operasjonelle nivået hvor en av hovedoppgavene nettopp er å planlegge og koordinere operativ aktivitet på tvers av domener for å oppnå maksimal effekt innenfor det fellesoperative konseptet. Man kan si at det fellesoperative området utvides, så også krav til kompetanse. Men fellesoperativt både er og må det være!

Refleksjon nummer to går mer i retning av begrepsbruken. Som sikkert mange vet, så pågår det kontinuerlig en operasjon i Norge, operasjon Joint Watch. Operasjonen har fokus på situasjonsforståelse i våre nærområder, hovedhensikten er å forstå hva som skjer, skille det unormale fra det normale og kontinuerlig opprettholde et godt beslutningsgrunnlag. Vår operasjonsprofil i området søkes å være av forutsigbar, fleksibel, fast og ikke eskalerende karakter. Med tanke på vår nabo i øst, som er en betydelig militær aktør i våre nærområder, så er akkurat det en fornuftig operativ profil for et lite land, særlig i forhold til den bilaterale relasjonen med Russland. Vår daglige operative profil i operasjon Joint Watch vil alltid være utgangspunktet for å håndtere eskalerende situasjoner over i krise, konflikt og i verste fall krig. Dersom begrepet Battle i MD BATTLE, indikerer at det nye konseptet er mer relevant i et høyere intensitets-scenario, så bør vi utvide begrepet i en mer omfattende retning, ta inn over oss hele operasjonsspekteret, kanskje MD Operations er mer passende begrep å benytte for oss.

Den tradisjonelle domenetilnærmingen med land, luft og sjø, er som nevnt utvidet med domenene space, cyber og elektronisk krigføring. Jeg tror at vi kollektivt har mer kunnskap om mulighetene og begrensningene i de tre første enn i de tre siste og nyeste. Dette krever justert fokus i utdanning, trening, øving, konseptutvikling og i utviklingen av planverk for å øke kunnskaps- og ferdighetsnivået, og den operative evnen. Dette må selvfølgelig også følges opp med kapasitetsutvikling til både forsvar og angrep. Det betyr en ytterligere kapasitetsutvidelse, ressurskrevende, men absolutt nødvendig. Noe av det

mest sårbare vi kan gjøre er å ikke opptre i, eller «konkurrere» i alle domenene. Fravær av egen eller alliert aktivitet i multi-domenene åpner en motstanders handlingsrom og øker egen sårbarhet. Utvikling og planlegging blir sentralt.

Hovedfokuset på operasjonelt ledelsesnivå er joint, eller fellesoperativ aktivitet, prioritering og synkronisering. Veldig, veldig forenklet dreier hovedprosessene seg om hva vi skal forsvare, Joint Defended Asset (JDA)-prosessen, og hva vi skal angripe med et utvalg av virkemidler, Joint Targeting (JTG)-prosessen. Understøttende fellesoperative prosesser er blant annet Joint Intelligence Surveillance & Reconnaisance (JISR) og Joint Battlespace Management (JBM). En erkjennelse av MDB, eller MDO som operativt konsept, stiller umiddelbart spørsmålet i JTG-prosessen, hva bør vi påvirke eller angripe? Noe annet enn det vi mer tradisjonelt gjør? Hvordan bør det angripes? Og hva er det mest egnede virkemiddelet? Tilsvarende vil spørsmålene rundt JDA kreve en revurdering av hva bør vi prioritere å forsvare, mot hva og hva er det mest effektive forsvarsvirkemiddelet? Det er ikke lengere sikkert at den beste måte å forsvare en digitalisert vannkraftbasert el-forsyning på er å fysisk bevokte små og store dam-anlegg og trafo-stasjoner. Kanskje ressursene er best benyttet i cyberdomenet.

En domeneutvidelse, fortettet stridsfelt, behov for å virke hurtig og presist på tvers av og sammen i de tradisjonelle og i de nyere domener krever et standardisert, interoperabelt og sømløst kommunikasjonssystem. Dette er et område med mange meninger og oppfatninger om hva som er riktig og hva som egner seg best. Jeg synes Sjef Cyberforsvaret redegjorde godt for det i sitt foredrag i går. Jeg registrerer en positiv utvikling mot nettopp standardisering, variantbegrensning og sikring av nettverk og kommunikasjon. Utfordringen er muligens tempoet vi i Forsvaret evner å gjennomføre dette i, særlig sett i forhold til tempoet i teknologiutviklingen utenfor Forsvaret. Mulighetene ligger muligens i å se hva kommersielle krefter evner å få til, og som raskt kan implementeres i våre militære systemer. Rask videreutvikling og tilnærmet kontinuerlig oppdatering av eksempelvis I-phone kan være et godt eksempel på det.

Et siste poeng som nok vil være sentralt for oss er å evne å se denne utfordringen med utvidede briller, ikke som en ren militær utfordring, men for oss også en betydelig samfunnsutfordring. Hovedårsaken til det er at vi gradvis, over tid og i stort omfang, har gjort oss mer og mer avhengig av det sivile samfunnet for å fungere. La IKT, logistikk og luftromskontroll stå som eksempler på det. Denne avhengigheten medfører at Forsvarets sårbarhet er mer lik samfunnets sårbarhet forøvrig. Positivt i dette perspektivet er det gode og fokuserte arbeidet med å videreutvikle Totalforsvaret. Det vil bidra til å øke samfunnets gene-

relle robusthet, og dermed også Forsvaret robusthet. Forsvaret er en integrert del av Totalforsvaret, ikke et uavhengig tillegg til Totalforsvaret.

Først og fremst krever det kompetanse for å bevege oss i en mer MDB retning, fordi vi må forstå, følge med og utvikle oss når vår viktigste allierte foretar konseptuelle dreininger i sine operasjonskonsepter.

Videre må vi tilnærme oss konseptet samtidig som vi ivaretar våre egne behov og egenskaper. Å endre forståelse fra MDBattle til MDOperations kan være et eksempel på det. Vi må benytte konseptet i forbindelse på pågående daglige operasjoner, økte ferdighetsnivået og skape et mer robust utgangspunkt for en eventuell eskalering. Det skjer i daglige operasjoner.

Nye viktige domener må sys inn og sammen, kommunikasjon i flere former er sentralt, det koster, men må prioriteres, å legge de relativt sett små pengene på de allerede store og kostbare prosjektene, for å oppnå store effekter, skaper mye operativ evne for lite ressursinnsats

Øke evnen til K2 i et ytterligere mer komplisert operasjonsmiljø krever ikke nødvendigvis mer trening, men en ny og annerledes tilnærming. Det samme gjelder for øvelser.

Vi må fortsette den gode og viktige jobben med å videreutvikle Totalforsvaret, og bidra til å øke de øvrige Totalforsvaraktørenes bevissthet rundt både avhengigheter og sårbarheter i de nye domenene.

Men, å tilpasse oss en ny fremtid vil vi lykkes vi med, rett og slett fordi vi allerede har mye flinke folk, fortsetter å utdanne nye, unge, smarte, oppegående, kritiske, lyttende og reflekterte soldater og medarbeidere, blant annet her på Luftkrigsskolen.

Luftforsvarets tilnærming til Multi-Domain Battle

av Aage Longva

I dette innlegget vil jeg gå nærmere inn på Luftforsvarets tilnærming til Multi-Domain Battle (MDB) og beskrive vårt behov knyttet til dette.

For Luftforsvaret er operasjoner i flere domener ikke noe nytt, men heller noe vi allerede er en del av. Luftforsvaret støtter i dag både landmakten og sjømakten, og således er vi en del av disse domenene, eller spesialområdene. USA bruker begrepene AirLand Battle og AirSea Battle, men MDB tar kanskje dette et steg videre. Flere domener innlemmes, og alle domenene skal sømløst virke sammen og samtidig.

MDB og F-35

Etter hvert som forståelsen av MDB utvides her hjemme, er det naturlig at Luftforsvaret utvider sin egen forståelse av det. F-35 vil i løpet av de neste årene utvikle seg til å bli ryggraden i Luftforsvaret og Forsvaret. Det nye kampflyet har evner og kapasiteter som langt overgår F-16. Vi vil snart kunne løse oppdrag på en annen måte enn vi kan med F-16, og vi kan påta oss nye oppdrag. Vi får en såkalt gamechanger, som kan operere nærmere motstanderens systemer, og vi kan stille opp i konflikter og trusselområder der F-16 i dag ikke bør komme for nær.

Bastionforsvaret er ikke lenger et uinntagelig fort, beskyttet av langtrekkende luftvern. Selv robuste, havgående marinegrupper, med seilende våpenplattformer som beskytter strategiske ubåter, er mål som nå kan nås. Krigsscenarioene kan altså utspille seg på en annen måte, og F-35 spiller en avgjørende rolle i dette. Men la meg være tydelig: F-35 vil ikke kunne løse oppdragene alene. Styrkesjefene og de til enhver tid støttende sjefene har unike kapasiteter som bidrar til fellesoperativ oppdragsløsning. Disse kapasitetene må brukes til det de er tilpasset og egnet for, og det samme gjelder F-35. Men det interessante er hvordan vi gjør hverandre gode.

F-35s kombinasjon av lav synlighet og avanserte, integrerte sensorer gjør det

mulig å gjennomføre hele «Find, Fix, Track, Target, Engage, Assess»-kjeden, uten assistanse utenfra. Det er imidlertid ikke sagt at det er ønskelig, eller noen ganger mulig. Havet er stort, og nordområdene likeså. For eksempel kan det være vanskelig å lokalisere stasjonære landbaserte eller fartøybaserte langtrekkende missil-launchere. Derfor er det sentralt at vi har en «Cross-Domain»-tilnærming, også for F-35.

Integrert forsvar

De andre luftmaktsystemene våre er også en del av denne helheten. Luftforsvaret har et sett av plattformer som dekker store områder når de gjennomfører oppgavene sine. Og dersom plattformer er riktig konfigurert, kan de samle inn informasjon og dele med helheten, men de vil også kunne løse egne oppdrag bedre ved hjelp av andre. Forsvarssystemer må kunne kommunisere sammen i et felles nettverk, med felles språk, slik at de kan bidra til en felles situasjonsforståelse og en felles sømløs målutvelgelsesprosess.

I løpet av de neste ti–femten årene vil store deler av Forsvarets kapasiteter bli skiftet ut. Nye ubåter, nytt luftvern og nye stridsvogner er eksempler på systemer som vil styrke Forsvarets totale slagkraft. Alene vil de kunne gjøre litt, men sammen vil de kunne gjøre mye. F-35 kan gjøre mye alene, men det er F-35s teknologisprang innenfor sensorkapasitet og utnyttelsen av dette som er et av kampflyets viktigste bidrag til Forsvarets fremtidige suksess. Nettverksfunksjonalitet i form av nettverksvåpen og utbygde Link-systemer gjør det mulig å bygge opp og dele situasjonsforståelse mellom fly og å integrere informasjon fra andre kilder. Men disse må kunne kommunisere sammen. De må håndtere et høyt graderingsnivå og dele informasjonen inn til et felles informasjonsbilde som er tilpasset brukeren. Systemene vi anskaffer, må være robuste multiplattformer, som om nødvendig kan fylle flere roller nærmest samtidig – «Swing-role». Sjef fagavdeling ved Hærens våpenskole, oberst Jan Frederik Geiner, har uttalt så treffende: «Systemene våre – å dele når vi kan og slåss alene når vi må».

Sjef Luftforsvaret har nevnt at MDB kan se ut til å ha likhetstrekk med storsatsingen nettverksbasert forsvar. Luftforsvaret har ønsket å utfordre seg selv på hvordan det kan utvikles i en MDB-kontekst. Gjennom taktikkprosjektet vi har gående sammen med Forsvarets forskningsinstitutt (FFI), utvikler vi verktøy for å kunne simulere Luftforsvarets kapasiteter og samspillet mellom disse. Prosjektet «Taktikk» ble startet for å få bedre grep på helheten i Luftforsvarets struktur og for å avdekke operative effekter av ulike tiltak som må gjøres med strukturen, samt for å optimere den operative innsatsen på tvers av ulike syste-

mer og prosesser i et kost–nytte-perspektiv. «Taktikk» har altså vært sentralt i utviklingen av et operasjonsoptimalisert Luftforsvar.

Vi ser at vi fortsatt har mye arbeid som gjenstår på Luftforsvarets hoveddomene: luftkontroll. Men vi har også tatt de første stegene med å vurdere våre nye systemer med en mer fellesoperativ tilnærming. Her er samarbeidet med FFI avhengig av et styrket samarbeid med andre grener eller domener på andre nivå. Så skal det bli interessant hvordan space-domenet blir en del av dette, og hva Luftforsvarets rolle knyttet til det blir.

Forsvaret har en vei å gå før vi har tatt MDB inn over oss. Vi må revisitere våre konseptuelle tankegods når det gjelder hva vi skal oppnå av effekter, og hvordan vi skal oppnå dem. Det handler kanskje ikke om en liten justering og finpuss av gamle og nåværende konsepter, men mer som en tydelig transformasjon. Til det behøver vi kompetanse, og gamle tanker må vike plass for nye. I kjøpet av F-35 spesielt har Forsvaret et ansvar for ikke å ende opp i en situasjon som om vi hadde kjøpt en Ferrari og brukte den til å kjøre til butikken for å kjøpe melk. F-35 er noe mer enn en litt forbedret versjon av F-16, og det å planlegge, lede og gjennomføre luftoperasjoner med F-35 som om det var en F-16, ville vært hverken militært hensiktsmessig eller økonomisk forsvarlig.

Avslutning

Avslutningsvis vil jeg si at Luftforsvaret er opptatt av å styrke gjennomføringsevnen sin, og at vi i samarbeid med FFI og andre domeneeiere kan komme frem til konkrete forslag og handlinger som gjør at våre fellesoperative ressurser ikke bare leverer tydelig i multi-domain-krigføring, men at dette også kommer det sivile samfunnet til gode gjennom våre daglige operasjoner. Fra anskaffelsesprosess til kampen på slagfeltet, enten det befinner seg på overflaten, under vann eller i luften, er det sammen vi gjør en forskjell.

Hærens syn på MDB

av Morten Jensen

Vi har i lengre tid fokusert på å knytte sammen sjø-, luft- og landdomenene for å optimalisere fellesoperasjoner nasjonalt. Modenheten vår vurderer jeg som god. Tanken bak Multi-Domain Battle er at vi evner å utnytte hverandres domener til å påføre en fiende tap, uavhengig av hvilket domene en selv opererer i. Multi-Domain Battle og Combat Cloud er konsepter som våre største allierte er i full gang med å ta frem. Cloud-prinsippet er brukt lenge i det sivile, og cloud computing er et kjent begrep.

Årsaken til at disse konseptene tas frem, er ønsket om å oppnå høyere tempo, større fleksibilitet og overlegen situasjonsforståelse i operasjonene. Hvordan kan vi i Norge få til et lignende konsept slik at sjø-, luft- og landmakt kan utøves dynamisk mellom alle nivåer og av alle kapabiliteter?

Sjø, luft, land – og sky

I et tidligere foredrag, oppfattet jeg at sjef Cyberforsvaret argumenterte for at Forsvaret må utnytte skytjenester til operative formål. Link-16 kan i dag støtte et slikt konsept, og vi i Hæren ønsker å sitte i førersetet når dette konseptet skal utvikles.

Hæren har erkjent at vi må satse mer på å dele den informasjonen vi har, med andre og bli bedre på å nyttiggjøre den informasjonen andre har. Combat Cloud-konseptet er et paradigmeskifte innenfor kommando og kontroll og gjør det mulig å automatisk koble sammen operative applikasjoner.

Hensikten med Combat Cloud-konseptet er å vri oppmerksomheten bort fra domenetenkningen og rette blikket mot fusion av all informasjon som er nødvendig for å bekjempe fienden.

Link-16 er meget resistent mot jamming, og vi har per i dag ingen andre driftssatte systemer som er bedre til å støtte informasjonsutveksling i sanntid. Vi må i tillegg ta frem en felles IKT-plattform med felles applikasjoner som støtter en felles targeting-prosess fra strategisk til stridsteknisk nivå. Ved å utnytte alle plattformer og enheter som sensorer vil vi bedre kunne utnytte de kapabilitetene som nye femtegenerasjons kampfly og andre kapabiliteter har og skal investere i, som CV90 & Strv. Godkjente targets må kunne gjøres til-

gjengelig for alle, slik at den som raskest mulig kan angripe målet, gjør nettopp det. Network Enabled Weapons blir en realitet om noen år, noe som også vil tvinge frem nye løsninger.

Langtrekkende presisjon

Våre nye kampfly, fregatter og korvetter har kapasitet til å beskyte flere mål samtidig, noe som vil medføre at det kan være mange våpen i ett og samme nettverk til samme tid for å mette en fiendes mottiltak. Dette sammen med Hærens kommende langtrekkende presisjonsvåpen vil tvinge frem mer robuste konsepter og nettverksløsninger. En trend vi ser, er at våpen- og sensorsystemer får stadig større rekkevidde – dette gjelder også for landdomenet.

Den vedtatte langtidsplanen vil gjøre Hæren mer relevant i alle domener. Materiellprogrammet til Hæren innebærer å investere i nytt rørartilleri med kapasitet til å bekjempe mål på 40 kilometers avstand. Om få år vil det være ammunisjon tilgjengelig for denne plattformen som øker rekkevidden til over 90 kilometer. Kampluftvernet vi anskaffer, vil utnytte AMRAAM-missiler fra NASAMS-systemet på Humvee-feltvogner (3 stk.) og IRIS-T missiler på panservognen M113 F4 (6 stk.).

Som et resultat av LMU ble det meget tydelig at KavBn/FLF må ha dedikert luftvernstøtte. Det blir derfor en økning av den allerede bestemte KLV-anskaffelsen. Vi etablerer EMT-kapasitet og planlegger å erstatte våre stridsvogner fra 2019. Sist, men ikke minst skal Hæren tilføres langtrekkende presisjonsvåpen med rekkevidde over 250 kilometer. Hærens evne til å lokalisere, velge ut og engasjere mål blir betydelig styrket og viser at vi kan bidra i alle deler av kill chain mot mål i alle domener.

En fordel landstyrker har, er at signaturen på nevnte plattformer er svært liten når de opererer på land, de er således vanskelige å oppdage, og det gjør plattformer på land mindre sårbare. Hærstyrker kan etablere midlertidig operativ handlefrihet for operasjoner i lufta og på sjøen ved å angripe motstanderens A2/AD-kapasiteter.

Langtrekkende ild er sentralt

Jeg ønsker å avslutte med et eksempel fra simuleringene som ble gjennomført i forbindelse med LMU. Av graderingshensyn har jeg valgt en annen geografi og tatt utgangspunkt i fienden som beskrevet i US ARMY TRADOCs «MDB – Evolution of Combined Arms for the 21st Century». Strukturen vi spilte med, var tilpasset og fremskrevet mot 2025 på begge sider.

Vi erfarer at fienden vil angripe strategiske, operasjonelle og taktiske mål fra flere domener samtidig. Luftvernet er hovedpilaren i A2/AD-kapasiteten og skal beskytte langtrekkende missilsystemer, maritime overflatefartøy og landstyrker. Motstanderen vil søke å skape asymmetri og utnytte rekkevidden han har i sine indirekte ildsystemer, jagerfly og elektronisk ild mot bakkestyrker.

Simuleringene indikerte at Hæren tidvis må klare seg uten støtte fra luft- og sjøstridskrefter. Hærens kapasitet til å projisere makt i luft- og sjødomenet er derfor avgjørende for fellesoperasjonen. Beskyttelse mot lufttrusler viste seg å være vesentlig i tillegg til evnen til målfatning. Langtrekkende ild er bærende for hele konseptet.

Egne stridsvogner og kampvogner viste seg å være effektivt til spesielt to forhold: å binde fienden og å tvinge frem mål gjennom egen manøver. Uten manøverstyrker trenger ikke motstanderen å eksponere HVT-ene sine. Bruken av kombinerte effekter (eller Multi-Domain) mot prioriterte og best beskyttede mål ga suksess, men fordrer fusion av targeting-informasjon for overlegen situasjonsforståelse og tempo i operasjonen.

Nye kapabiliteter og ny landmaktstruktur vil gi nye operative kapasiteter som vi nå må evne å utnytte ikke bare grenvis, men sammen i en Combat Cloud. En fungerende targeting-prosess med riktige verktøy som kan gi våre nye våpen CAT 1-koordinater, vil kunne påføre en fiende betydelige tap i en tidlig fase av operasjonen.

Multi-domene gjelder alle

av Nils Andreas Stensønes

Fra Sjøforsvarets perspektiv har vi tenkt mye på Joint- og nettverksbasert krigføring. Nå begynner vi å lese om Multi-Domain Battle, hvor vi ser både likheter og forskjeller. Men jeg tror det viktigste er at dette er en ny måte å tilnærme seg en problemstilling på – ikke en problemstilling som er ukjent, men som settes i en annen kontekst og blir belyst fra en annen vinkel. Jeg tror det kommer til å bringe noen nye erkjennelser. Spesielt for min egen del ser jeg at det setter en del ting som har ligget der, og som jeg har lurt og grublet på, inn i et rammeverk som har vært veldig nyttig.

La meg begynne med noen konstanter. Det er viktig å huske på at verden utvikler seg, men at det fortsatt vil være noe som er konstant. Vi er en arktisk nasjon, og vi har suverene rettigheter og plikter over et enormt havområde. Vi er plassert med tilgang til Nord-Atlanteren, arktiske kommunikasjonslinjer og store ressurser. For det tredje er vi NATOs flanke i nord og naboen til en stormakt som har interesser i nærområdet vårt. Videre har vi en litt spesiell situasjon hva gjelder geografien – 85 prosent av området vårt er hav, og 100 prosent av det er dekket av luft og space. Jeg vil påstå at det største problemet med dette er at norsk territorium befinner seg innenfor Russlands A2AD-boble. Hvorvidt den er satt eller ikke, er ikke så interessant med tanke på våpnene og systemene som våre venner i øst har. De er der nå. Da er vi i en situasjon hvor vi er nødt til å kunne beskytte suvereniteten vår og operere innenfor denne boblen. Vår evne til å gjøre det vil bli truet fra verdensrommet, fra luften, det elektromagnetiske spekteret, cyber, fra land og fra både over og under vann.

Admiral Harry B. Harris Jr. ved US Pacific Command (PaCOM) holdt et foredrag om dette temaet: «Gjennom brorparten av historien har det eneste domenet vi virkelig har blitt bestridt i, vært landdomenet. Vi har hatt handlingsfrihet i luft-, rom-, maritim- og cyberdomenene. Det har vært spesielt tydelig de siste femten–tjue årene. Men det vil ikke være sånn i fremtiden. Vi må nok forvente at en motstander vil etablere en kampanje som er orkestrert i alle disse domenene. Han tenker nok som oss og kommer til å bruke alle disse domenene effektivt. Han kommer til å bruke hele sin stats virkemiddelapparat – fra helt nederst på Soft Power-skalaen, til hele veien opp til det ultimate Hard Power.»

I vårt nærområde ruster Russland opp med det som er spesielt nytt: langtrekkende presisjonsvåpen levert fra fly, overflate og særlig fra undervannsbåter. Gjennom dette innlegget kommer jeg til å benytte ubåter og undervannsdomenet som eksempel for å illustrere effekter vi kan ha en multidomene-tilnærming til. Utfordringen med ubåter er å lokalisere de. Den andre utfordringen er at de kan utgjøre ulike trusler. Det kan være offensivt. Det kan være innsetting av spesialstyrker. Det kan være utplassering av sensorer. Det kan være å påvirke infrastrukturen på havbunnen. (Det er interessant å legge merke til at 95 prosent av det som gjøres på en smarttelefon over internett, går gjennom fiberoptiske kabler på havbunnen. Jeg tviler på at disse får være i fred under en konflikt.) Dette er et forferdelig ressurskrevende domene, og derfor er vi nødt til å tenke litt spesielt på det. Å bekjempe en sånn type trussel tror jeg vi gjør smartest hvis vi tenker multi-domene eller Joint, litt avhengig av hvordan vi velger å se på det.

Sjøforsvarets oppgave er å sikre havområdene for egen bruk i fred, krise og krig og å sikre mottak av allierte. Til det sistnevnte trenger vi disse havområdene, da det tunge materiellet kommer sjøveien. Vi må sikre vår evne til å operere effektivt under truslene som er beskrevet. For oss er vi NATO i nord, og der har vi et spesielt ansvar. Vi må bidra til det som kanskje er den største utfordringen vi har akkurat nå, og det er kontrollen i undervannsdomenet. Dette har NATOs generalsekretær Jens Stoltenberg understreket i flere taler. Videre er det en signifikant endring fra den kalde krigen. Da hadde begge sider et stort volum, og vi var svært defensive taktisk sett. Nå har begge sider et vesentlig mindre volum, som betyr at vi er nødt til å bruke det vi har, på mye smartere måter, og effekten vi får ut av smart bruk, vil være proporsjonalt mye større. Jeg tror nye kapabiliteter og multidomene-operasjoner vil fordre en taktikkendring. Det vil medføre høyere tempo, og ikke minst endringer i kommando og kontroll, samt trening og øving.

Forsvaret i bredden

La oss ta for oss kommando og kontroll først. Fundamentet vårt for samhandling er effektiv kommando og kontroll. Her må vi få mye mer ut av den nye kommandostrukturen vår, der vi som grensjefer er nødt til å ta ansvar og bygge kompetansemiljøer på tvers av grenene og domenene. Etter hvert som multidomene-operasjoner tiltar, vil det stille større og andre krav til fellesoperativt nivå med hensyn til hva og hvordan vi synkroniserer innsatsen. Men ikke minst forventer jeg at mer må gjøres på taktisk nivå. Det betyr at vi også må tenke multidomene – på tvers av alle grener. Man er nødt til å tenke: «Hvordan kan

jeg bidra i alle domener?» Vi kan ikke overlate denne synkroniseringen ene og alene til Forsvarets operative hovedkvarter (FOH), det tror jeg ikke er hensiktsmessig. Det betyr at vi må tenke fellesoperativt, som det het før, og nå Joint eller multidomene, fra strategisk nivå hvor alle statens virkemidler synkroniseres, til det operasjonelle nivå hvor vi synkroniserer alle grenene, og ned på det taktiske nivå hvor vi bruker alle ressursene vi har i de ulike domenene, for et mer begrenset mål. Det betyr faktisk at vi alle må tenke multidomene. Vi må først tenke på hva det er vi skal beskytte, for motstanderen kommer til å operere på samme måten. De fleste trusler vi står overfor, er umulig å løse hvis vi bare håndterer dem i én dimensjon eller i ett lag. Her tror jeg det er nødvendig med ikke bare det gode, gamle begrepet «Forsvaret i dybden», men også Forsvaret i bredden, som multidomene-tenkning jo egentlig er. La meg ta et eksempel: Det er lite poeng i å stå i kringvern rundt en K2-node hvis angrepet kommer via cyber eller som kryssermissiler. På tvers av grenene må vi jobbe for å finne de gode løsningene. Det vil fortsatt være kamp mellom grenene om ressurser, men vi er nødt til å forstå at de andre grenene kan hjelpe oss ganske kraftig.

Den offensive operasjonen i multidomene

La meg igjen begynne med et eksempel fra undervannsdomenet. Motpartens ubåter er vanskelige – har de først dykket, vet vi ikke hvor de er. Hvordan bekjemper vi en slik trussel? Vi er selvfølgelig nødt til å tenke hvor sårbarhetene hans er, som sannsynligvis er før han dykker. Derfor pleier jeg å terge antiubåtmiljøet i Sjøforsvaret ved å si at det beste AU-platformene vi har i dag, er F-16 med presisjonsvåpen, og i fremtiden F-35 med JSM. Da blir det litt uro i salen inntil jeg sier at jeg mener at vi må ta den før ubåten seiler fra kai. Det er da vi vet hvor den er, og hvor vi kan gjøre noe med den. Igjen: Vi må bruke de andre domenene for å påvirke fienden der han er sårbar. Lykkes vi ikke med det, er det skrekkelig vanskelig å finne ubåten. I så fall må vi tenke annerledes, for eksempel: Hvordan kan vi gjøre våpnene hans mindre effektive? Hans langtrekkende våpen er avhengig av posisjonering, som benytter seg av GPS eller GLONASS. Kan dette påvirkes ved hjelp av Cyberforsvaret? I så fall trenger jeg kanskje ikke så voldsomt med luftvern på Haakonsvern for å beskytte logistikken min, fordi våpenpresisjonen hans blir såpass redusert gjennom bekjempelse i et annet domene.

Multidomene på alle nivåer

Poenget er at alle kapasiteter må settes i system med en taktikk som ikke bare beskriver Forsvaret i dybden, men også i bredden. Oppsummert forventer jeg at en multidomene-tilnærming vil styrke evnen til å kjempe effektivt, beskytte det vi har, effektivt, og angripe det vi skal angripe, effektivt. I tillegg er vi nødt til å tenke multidomene på alle nivåer – på strategisk, bruk av alle statens virkemidler; det operasjonelle nivået, som vil si synkronisering av hele Forsvaret; det taktiske nivået, som innebærer synkronisering av enkeltkapasiteter for å løse konkrete oppdrag. Sist, men ikke minst må vi gjøre dette alle sammen, også vi som er nede på taktisk nivå, samt skipssjefene der ute.

Cyberforsvarets perspektiv på Multi-Domain Battle

av Inge Kampenes

Introduksjonen av et nytt operativt domene i Norge og NATO, cyberdomenet, legger til et ekstra perspektiv i militær operativ tenking. Denne teksten er et forsøk på å forklare cyberdomenet i konteksten av Multi-Domain Battles (MDB) og derigjennom Cyberforsvarets syn på det sistnevnte.

Det er viktig å erkjenne at det er to store temaer vi berører. Begge temaene er også i betydelig utvikling og endring og vil utvikle seg videre og modnes i årene som kommer. Det er heller ikke slik at vi, når vi samles, har felles og omforente perspektiver på hva cyberdomenet er, og hvilke utfordringer og muligheter det gir oss, ei heller hva som er de viktigste tankene omkring Multi-Domain Battles.

La oss starte med Multi-Domain Battles – eller MDB. Slik jeg ser det, er det en viktig erkjennelse, som jeg har argumentert for tidligere, at vi befinner oss i en verden i hurtig teknologisk endring. De teknologiske paradigmeskiftene i samfunnet rundt oss inntreffer hyppigere i dag enn på noe annet tidspunkt i historien – og utviklingen akselererer eksponentielt.

Samtidig er vi, som militære organisasjoner, tradisjonelt dårlige på å følge denne typen galopperende utvikling som den fjerde industrielle revolusjon utgjør. Vi er vant til å bruke lang tid på å utvikle revolusjonerende teknologi, introdusere den til slagmarken og så benytte denne teknologien i flere tiår, i beste fall med noen begrensede mid-life updates i løpet av materiellets levetid.

Det betyr at over levetiden til én generasjon militært kjernemateriell, som typisk er 20 til 30 år, så vil flere teknologiske generasjoner passere. Materiellet vil, for å si det enkelt, bli teknologisk akterutseilt raskere.

I disse teknologiskiftene introduseres også nytt materiell i det sivile, som potensielle motstandere kan ta i bruk, noe som gjør at de tradisjonelle store militærmaktene ikke lenger kan forutsette å være teknologisk ledende og dominerende på alle domener. Jeg tror det er den viktigste erkjennelsen for USA når det gjelder MDB. For å fortsette å dominere slagmarken, eller Battle Space som helhet, er det nødvendig å være dyktigere enn motstanderen til å utnytte

effektorer fra flere domener inn mot samme mål eller operasjonslinje – for å opprettholde dominans i tid og rom.

I dette perspektivet har kanskje ikke MDB veldig mye nytt å bringe til Forsvarets militære tenking. Vi har aldri vært der at vi har tenkt å dominere i enkeltdomener. Satsingen vår har vært på samvirke og fellesoperasjoner all den tid teknologien har åpnet for det.

Vi må, naturlig nok, kontinuerlig styrke evnen til å få et lite Forsvar til å virke sammen, og vi må styrke evnen til både samvirke og felles planlegging med NATO. Men i dette perspektivet er MDB – for Norge – mer en videreføring av samvirke- og fellesoperasjonstankegangen enn en radikalt annerledes måte å tenke på.

Cyberdomenet har flere sider ved seg som det er verdt å dvele ved når vi snakker om MDB. På den ene siden er cyberdomenet en forutsetning for moderne militære operasjoner – altså en *enabler*.

Videre tjener domenet en viktig funksjon når det gjelder synkronisering av operasjoner og effekter, og for ledelse og styring av militære operasjoner, altså kommando og kontroll.

Domenet vil også kunne være en viktig styrkemultiplikator i det at den aktøren i Battle Space som evner å utnytte digitalisering og det nye domenet mest effektivt til sine operasjoner, vil høste en betydelig gevinst sammenliknet med andre aktører.

Det gir oss selvsagt også en mulig angrepsvektor hvor vi kan redusere motstanderens operative evne og gi oss overlegenhet på land, til sjøs eller i luften – avgrenset i tid og rom.

Så følger det selvsagt også utfordringer med voksende digitalisering og en skyggeside knyttet til vår avhengighet av det nye domenet. Etterretningsmessig vil en motstander få betydelige muligheter til å hente ut informasjon om styrkene og planene våre – ikke bare fra våre nettverk og systemer, men også fra samfunnet, som digitaliseres rundt oss.

Vår avhengighet av domenet gir oss også en operativ sårbarhet i det at vi etablerer kjerneprosesser og funksjonalitet som kan påvirkes og degraderes, og dersom motstanderen lykkes med dette, vil det redusere den operative evnen vår.

Sist, men ikke minst blir de digitale systemene og teknologien vi tar i bruk, en angrepsvektor for en militær motstander, hvor de kan høste operative fordeler ved å ramme sambandssystemer og plattformer og i praksis redusere vår operative evne og slagkraft.

Skal vi tenke MDB i et effektperspektiv, vil militære planprosesser bli mer komplisert i fremtiden – som følge av at man må planlegge effekter i detalj og

synkronisere dem i flere domener. Men, og her ligger det originale eller nye sett fra mitt perspektiv: MDB kan være en viktig katalysator for å få større konsentrasjon om, og raskere forståelse for, effekter i cyberdomenet, fordi konseptet inviterer cyberoperasjoner inn som en opsjon for de operative planleggerne fra første stund.

En slik utvikling vil få konsekvenser med tanke på kompetanse. For å forstå effektene fra flere domener, og å kunne spille på slike effekter, må fellesoperasjonstenkingen inn på et stadig lavere nivå i utdanningen vår. Her tror jeg, oppriktig, at den nye utdanningsreformen vil kunne gi oss fordeler ved å sikre at unge offiserer og spesialister på et tidlig tidspunkt får forståelse for og kunnskap om mulighetene og avgrensningene som andre domener kan tilby. Spesialistkorpset i seg selv vil være en fordel siden man får stabil erfaring på lavere nivåer, og man får en faglig stabilitet og ballast som støtte til unge sjefer på lavere nivåer.

I de operative planstabene på høyere nivåer må vi ha kjennskap til hvilke evner og forutsetninger de forskjellige domenene representerer i Battle Space. For å kunne planlegge for effekter, se mulige følgekonsekvenser og forstå hvordan effektene kan virke inn på hverandre, må man ha detaljert innsikt i alle domener. Man må vite hva som er mulig å få til, og hvilke kapasiteter den enkelte aktør besitter. Jeg tror erkjennelsen og utviklingen av MDB i Forsvaret vil innebære en vesentlig satsing på plankapasiteten i FOH.

For å høste mest mulig effekt av tankene bak MDB vil det være nødvendig også å evne å se alle fem domenene i sammenheng og opprette og utnytte mulighetene som ligger der hvor domenene kan virke inn over hverandre. Ved å utnytte styrkene som ligger til det enkelte domene, for å redusere svakhetene og sårbarhetene i de andre – og ved å evne å fullt ut utnytte sensorer og effektorer på tvers av domenegrensene; da kan vi høste betydelige gevinster i operativ sammenheng.

Avslutningsvis våger jeg påstanden at det domenet som er minst modent blant verdens militære aktører, er cyberdomenet. Det fører med seg noen utfordringer. Men det betyr også at i et Multi-Domain Battles-perspektiv vil den nasjonen som raskest evner å høste de mulige gevinstene av det nye domenet, og som evner å synkronisere cybereffekter med effekter fra andre domener i Battle Space, kunne høste betydelige operative fordeler.

Space i et multi-domain perspektiv

av Stig E. Nilsson

Først vil jeg berømme Luftforsvaret for å være den første norske forsvarsgren som inkluderer Space-domenet som en del av diskusjonen om fremtidens forsvar. Timingen er meget god, siden både Stortinget, regjeringen og forsvarssjefen anerkjenner Space som strategisk viktig for Norge generelt og for Forsvaret spesielt.

Fra starten av Space-æraen for drøye seksti år siden til for en drøyt ti–femten år siden var rommet et fredelig domene, primært for sivil og i tilfelle militær utforskning.

Space har til alle tider fascinert og inspirert både vanlige mennesker, kunstnere, gründere og nasjoner. Også Norge har hatt sine tidlige pionerer på 60-tallet. Odd Dahl ved Forsvarets forskningsinstitutt (FFI) var en av våre gründere på dette området. Vi kaller denne epoken «Old Space».

«New Space»

I dag er Space annerledes. Teknologisk utvikling og kommersiell satsing har åpnet nye dører til rommet. Utviklingen av billigere, men likevel svært kapable småsatellitter har siden tidlig på 2000-tallet gjort Space tilgjengelig for mange nye aktører og nasjoner, også Norge. Vi kaller denne nye epoken «New Space». New Space-satsingen har ført til en voldsom økning i antallet satellitter. Denne nærmest eksplosive økningen i antallet satellitter, kombinert med en mangel på internasjonalt aksepterte romlover, har resultert i at vi i dag anerkjenner space-domenet som «Congested, Contested and Competitive». Utviklingen innen New Space vil medføre at romdomenet blir stadig viktigere, både sivilt og militært. Space-kapasiteter har utviklet seg til å bli en forutsetning for de fleste våpensystemer og militære operasjoner. Space-systemer er av natur systemagnostiske; de støtter alle domener. Men de trenger også beskyttelse fra alle domener. I et Multi Domain perspektiv er dette sannsynligvis et vesentlig poeng.

Jeg vil kortfattet dekke de tre mest aktuelle områdene innenfor «Space Force Enhancement». Det første er Posisjon, Navigasjon og Tid (PNT), eller Gobal Navigation Satellite Systems som det benevnes internasjonalt. Det andre er jordobservasjon, og det tredje er satellittkommunikasjon.

Space Domain Awareness (SDA) og Space Situational Awareness (SSA) er områder som vil få økt oppmerksomhet og betydning for Multi Domain operasjoner i tiden fremover, men dette temaet får vi heller komme tilbake til ved en annen anledning.

1 Global Navigation Satellite Systems (GNSS)

I dag er samfunnet vårt avhengig av *Global Navigation Satellite Systems (GNSS)*, slik som GPS og det kommende europeiske systemet Galileo. Børser, minibanker, mobiltelefoner miljøovervåkning og ikke minst pizzalevering ville fungert like dårlig som klister på nysnø uten tilgang til GPS. Siden den første Golfkrigen har de fleste av våre moderne våpensystemer i økende grad blitt avhengige av GPS. Enten for presisjon, tidssynkronisering eller navigasjon. Eksempelvis er 70 prosent av alle våpen i US Army i dag avhengig av GPS. Jeg tror Norge i økende grad også går i samme retning. GPS er derfor en kritisk kapasitet for alle militære operasjoner. Men denne avhengigheten innebærer også at disse systemene er en potensiell akilleshæl.

2 Jordobservasjon

Det andre området for Space-bidrag til Multi Domain-operasjoner er jordobservasjon. Det er særlig innenfor jordobservasjon at New Space-kapabiliteter er mest fremtredende. Kommersielle systemer tilbyr i dag elektrooptiske og ugraderte bilder med en oppløsning ned til 25–30 centimeter, til en brøkdel av kostnadene ved Old Space-systemer. Jordobservasjon er viktig av minst tre grunner: For det første gir det rask tilgang til høyoppløselige bilder, både for strategisk, operasjonelt og taktisk nivå. For det andre gir det verdifull og hyppigere oppdaterte data for «Intelligence, Surveillance and Reconnaissance»-oppdrag (ISR). Og for det tredje vil rombasert overvåkning bli en mer kosteffektiv metode for de fleste overvåkningsoppdrag.

3 Satellittkommunikasjon

Det tredje innenfor «Space Force Enhancement» er satellittkommunikasjon. Moderne plattformer genererer mye data og trenger mye data. Innsamlede data må ideelt sett videreformidles i løpet av sekunder, i stedet for minutter eller timer, som er normalen i dag. Satellittkommunikasjon er i dag den eneste effektive metoden for «Beyond Line-Of-Sight»-bredbåndskommuni-

kasjon (BLOS), og som sådan en kritisk ressurs for effektive og synkroniserte operasjoner. I Norge har vi vært begrenset av mangelen på robuste muligheter for satellittkommunikasjon i nord. Dette henger sammen med at bredbåndskapable satellittkommunikasjonssystemer er satt i geostasjonær bane. Men dette vil sannsynligvis endre seg innen få år. I et Multi-Domain perspektiv er robust og sikker tilgang til bredbånds satellittkommunikasjon viktig for effektiv kommando og kontroll, og en forutsetning for at våpensystemer skal fungere optimalt i en fellesoperativ kontekst.

Sårbarhet

Til tross for en global, uforutsigbar og volatil sikkerhetssituasjon er Space et domene som forutsigbart vil tilby nye kapasiteter og akselerert vekst. Dette vil øke spekteret og tilfanget av tjenester og skape større robusthet og sikkerhet for kritiske Space-kapasiteter til Multi-Domain operasjoner.

Imidlertid er internasjonalt samarbeid og internasjonalt aksepterte lover avgjørende for å hindre ukontrollert vekst og potensielt kaos i Space. Vår økende Space-avhengighet skaper en tilsvarende sårbarhet og sikkerhetsutfordring, både for samfunnet og ikke minst for våre moderne styrker. Denne åpenbare sårbarheten og sikkerhetsutfordringen bør ikke undervurderes. Anerkjente Space-eksperter har allerede uttalt følgende: *Det er ikke et spørsmål om det blir krig i Space, bare et spørsmål om når.*

Hvordan vil Multi-Domain Battle-konseptet påvirke Luftforsvaret?

Fra «tripwire» til «Norge er NATO i nord!»[1]

av Jens Gunnar Haugen Dragsnes

(Teksten er basert på et foredrag som ble holdt på sjef Luftforsvarets Luftmaktseminar 8. februar 2018.)

Innledning

På årets Luftmaktseminar har vi blitt kjent med begrepet Multi-Domain Battle (MDB). Vi har fått beskrevet den internasjonale konteksten konseptet har vokst frem fra: et Russland og et Kina som har studert USAs og NATOs operasjoner i Irak, Afghanistan, Libya og Syria. Et Russland og et Kina som har blitt skremt av effekten vestlige operasjoner har hatt, og som ikke ønsker slike operasjoner benyttet mot dem. Et Russland og et Kina som har investert i nytt materiell innen missilteknologi, luftvern, cyber, EK, flystyrker, satellitter og flåtestyrker for å håndtere moderne vestlige styrker.

Men hva betyr Multi-Domain Battle-konseptet for Luftforsvaret? Sjef TRADOC i US Army, General Perkins[2], er opptatt av at man må stille de riktige spørsmålene for å forstå en kontekst og en utfordring. Jeg ønsker derfor å starte med noen spørsmål knyttet til hva MDB kan bety for Luftforsvaret: Hva betyr e-tjenestens utsagn om at varslingstiden vår er redusert,[3] kanskje fra

1 Ine Eriksen Søreide 6. oktober 2016. https://www.facebook.com/Forsvarsdep/videos/14788684-18806196/

2 General Perkins er i sin rolle som sjef TRADOC US Army en av hovedarkitektene bak begrepet Multi-Domain Battle.

3 FOKUS 2018. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.

måneder, som vi mente vi hadde før 2014, til timer nå i disse dager?[4] Og tenker vi å ta oss råd til å sette luftvernet vårt på 15 minutters beredskap slik vi har F-16 på 15 minutters beredskap? Bør alle bransjene i femtegenerasjons Luftforsvaret bli «stealthy», drive «sensor fusion» og ikke minst være manøvrerbare?[5] Trenger vi å utvide begrepet «Recognized Air Picture» (RAP) til også å omfatte droner og «Recognized Space Picture»? Hvordan utfører vi multi-domain-kommando og -kontroll? Hvilken betydning har autonome operasjoner for Luftforsvarets kommando og kontroll i MDB? Hvordan utfører vi multi-domain-investeringer i Forsvaret? Er det på tide å gjeninnføre operative evalueringer (OPEVAL) i regi av NATO for i det hele tatt å kunne kvalitetssikre kampevnen vår i et MDB-scenario? Det er mange flere spørsmål man kan stille seg om temaet. Jeg har valgt ut to som jeg ønsker å belyse nærmere basert på hva jeg mener er hovedtrendene i diskursen i Luftforsvaret i dag:

1 Hvordan skal Luftforsvaret unngå å bli nøytralisert i en tidlig fase av en konflikt og dermed de facto eliminert fra MDB?
2 Hvordan utfører vi multi-domain kommando og kontroll?

Sitatet fra Søreide i underoverskriften er med på å tydeliggjøre viktigheten av at vi som NATO-nasjon tar multi-domain-fellesoperasjoner alvorlig. Dersom det norske Forsvaret bare skal være en «tripwire», trenger vi ikke å utøve noen særlig operativ effekt på en eventuell angriper. Små ukoordinerte norske avdelinger trenger bare å blø nok til at NATO tar i bruk artikkel 5 og sender hjelp. Imidlertid vil en erkjennelse av at vi er NATOs nordflanke med et geografisk ansvar, stille større krav til den militære effekten de norske styrkene skal ha på en eventuell angriper. Evnen til å kjempe i komplekse fellesoperasjoner med høy intensitet vil være avgjørende for vår rolle som respektabel NATO-nasjon.

Konklusjonene på de to spørsmålene jeg har valgt, skal jeg ta med en gang. Så får vi ta argumentasjonen og begrunnelsene etterpå.

4 Søreide (2016). Tale i Oslo militære samfund.
5 Hva som regnes som femtegenerasjons egenskaper, er omstridt, men noen av egenskapene som omtales, er: stealth, «supercruise» (evne til å fly supersonisk uten bruk av etterbrenner), supermanøvrerbarhet, moderne sensorer og «sensor-fusion» for bedre situasjonsoversikt samt nettverksegenskaper. Se for eksempel: https://en.wikipedia.org/wiki/Fifth-generation_jet_fighter#Critics_and_alternative_definitions

1 Luftforsvaret må utvikle et system av systemer for beredskap, kampevne og utholdenhet. Det finnes ikke en «Silver Bullet» som enkelt og billig løser alle disse utfordringene!
2 Luftforsvaret må ta ansvar for å utvikle multi-domain-kommando og -kontroll med de øvrige forsvarsgrenene og ikke fokusere for mye på autonome operasjoner med F-35!

Hvordan skal Luftforsvaret unngå å bli nøytralisert i en tidlig fase av en konflikt og dermed de facto eliminert fra Multi-Domain Battle?

Multi-Domain Battle-konseptet sier at man skal kunne presentere en motstander for ulike multi-domain-utfordringer/-dilemma for å forvirre og nøytralisere. Det forutsetter selvfølgelig at forsvarsgrenene har manøvreringsevne og ikke allerede selv er slått ut eller nøytralisert. Vi har i det siste sett oppslag i media om at Ørland og Evenes mangler langtrekkende luftvern. Norsk luftvern er endelig kommet tilbake i rampelyset etter å ha vært på kanten av utryddelse i mange år. Og dette til tross for at andre land som USA, Russland og Kina har satset tungt på luftvern og missilforsvar i hele perioden. Jeg mistenker at det er «arven» som har lurt oss inn i tankegangen om at luftvern ikke bør prioriteres, og som fremdeles rir Luftforsvaret som en mare også på andre områder. Ikke «arven fra den kalde krigen», men «arven fra perioden 1990–2014». Perioden da vi mente vi ikke hadde noen trussel mot våre baser, styrkene i Afghanistan alltid hadde luftherredømme over seg, og Vesten hadde monopol på langtrekkende presisjonsvåpen. En hel generasjon offiserer og befal er vokst opp og utdannet i denne perioden.

Mange offiserer argumenterer for at nå har vi jo fått modernisert nesten hele flyparken, vi kan ikke be om mer penger nå. Da må noe annet ut! Men må det egentlig det?[6] Vi har hørt utsagn som: «Luftforsvaret må velge mellom fly eller baser! Nå har Hæren redusert til to baser, og Sjøforsvaret har redusert til én base. Nå er det Luftforsvarets tur å redusere til én base.» Og det har Luftforsvaret klart. I 2012 ble det besluttet at Ørland skulle være en kompakt base for styrkeproduksjon, og Evenes skulle ha QRA. Men i 2014 skjedde det en markant endring som politikere i Norge, og offiserer, sliter med å akseptere. Annekteringen av Krim og angrepet på Ukraina har gjort at man på nytt

6 https://www.vg.no/nyheter/innenriks/i/L01KXJ/nye-tall-norge-bruker-lavere-andel-p%C3%A5-forsvar-i-strid-med-nat-os-m%C3%A5l

må ta hensyn til den styrkede spenningen mellom Russland og NATO. Selv om de fleste i Forsvaret skjønner at det er en «ny normalsituasjon i Nord»[7], som Forsvarssjefen (FSJ) sa i Oslo Militære Samfund (OMS) nå i januar, så sliter vi med å akseptere de økte kostnadene en slik erkjennelse medfører. Vi leter etter den ene «Silver Bullet», eller mirakelkuren, som skal løse trusselen fra Russland **samtidig** som man opprettholder dagens lave kostnader. Denne «Silver Bullet» var først F-35, men så har man innsett at dersom F-35 er «så godt som usårbar» i lufta, så vil jo enhver skjønne at man må nøytralisere disse flyene på bakken! Flyet er absolutt ikke en gamechanger når den står på bakken!

Nå har vi kommet opp med enda en «Silver Bullet»: langtrekkende luftvern. Vel og bra er det at luftvern har fått mer oppmerksomhet, og at det er besluttet å anskaffe langtrekkende luftvern, men det er nok heller ikke nok hvis vi tar på alvor at vi skal forberede oss på konflikt med «near-peer adversaries».[8] Og det er her problemet med «arven» ligger nå. Hva hvis vårt svært begrensede luftvern ikke rekker å komme til skudd, eller noen kryssermissiler eller taktiske ballistiske missiler (TBM) slipper gjennom «luftvernnettingen» (jeg unnlater å kalle det en luftvernparaply før jeg ser at vi har et konsept med mengde, miks og mobilitet)? Nå er ikke problemet med de sårbare stasjonære basene i Norge noe nytt. F-16 trente på å operere fra kortbanenettet frem til cirka år 2000 i tillegg til at man opprettholdt flere deployeringsbaser. Det er ikke slik at jeg mener at vi skal opprettholde baser over hele landet, men det bør være mulig å tenke seg et konsept med større mobilitet til å kunne ta i bruk sivile flyplasser med deployerbar ammunisjon, vedlikehold og personell. Finland, Sverige og også Hviterussland har fortsatt opprettholdt sitt konsept på dette. Luftforsvaret har ikke klart å kommunisere tydelig nok en av Luftforsvarets grunnleggende forskjeller fra Hæren og Sjøforsvaret.[9] For mens Hæren setter i marsj ut fra garnisonene og ut i felt for å slåss og bo i telt, og Sjøforsvaret legger fra kai ved Håkonsvern og ut i fjorder og hav og sover på båt, må Luftforsvaret slåss fra basene sine. Og basene ligger dønn i ro! Det er ikke bare å rulle flystripa sammen og flytte. Det virker nå som om til og med vi i Luftforsvaret tviholder på ideen om basene våre som den godt befestede Maginotlinjen, til tross for at våre motstandere og vår viktigste alliert (USA) åpenbart går for «Blitzkrieg»-

7 https://www.oslomilsamfund.no/foredrag-forsvarssjefens-arlige-statusoppdatering-gjennomforingsevne-og-modernisering/

8 Begrepet brukes i USA som beskrivelse på en eventuell konflikt med Russland og Kina.

9 Selv om det i FFOD presiseres at en av svakhetene til luftstyrker er baseavhengighet. (FFOD s. 112)

konseptet! Når til og med US Air Force kommer opp med at de må kunne forberede seg på å operere fra mer spredte og små flyplasser, bør kanskje også Norge vurdere dette på nytt.[10]

Nå er det ikke slik at jeg forventer et russisk angrep, men jeg ønsker at vi skal ha et konsept som virker og er troverdig. Nå oppleves det ikke slik. Våre offiserer og befal må ha tro på at konseptet kan virke. Et konsept med F-16 og F-35 som opererer uforutsigbart fra sine faste baser med luftvern med riktig mengde, miks og mobilitet, god kamuflasje og narretiltak («decoys»), EOD og Rapid Runway Repair (RRR). Baser som kan drive utstrakt elektronisk krigføring av både radarsignaler, GLONASS/GPS, droner samt blender angriperes elektrooptiske kamera med laserstråler («Dazzling»)[11]. Et konsept hvor våre flybasers Force Protection er i stand til å håndtere moderne luftlandeavdelinger. Et konsept hvor til og med dette ikke er nok, men hvor personell og materiell kan ta i bruk sivile flyplasser i hele Norge for å reise seg opp igjen og slåss videre etter et første overraskende angrep. **Et helhetlig konsept er det som skal til for å avskrekke en fiende. Ikke sterke enkeltkapasiteter med store sårbarheter i støttestruktur.** Et konsept hvor NAOC ikke bare kan lede striden fra sin faste infrastruktur, men ta i bruk mobile hovedkvarter. Amerikanerne ser behovet for en dreining fra store stasjonære og signatursterke hovedkvarter til mer små, mobile og «stealthy» hovedkvarter som sentralt i Multi-Domain Battle mot jevnbyrdige motstandere («peer adversaries»). Store stasjonære hovedkvarter og sensorer med stor elektromagnetisk signatur vil raskt bli lokalisert og slått ut. Hvordan skal vi da drive «multi-domain» kommando og kontroll?

«Multi-domain» kommando og kontroll: Autonome operasjoner?

Dermed har begrepet autonome operasjoner igjen havnet i søkelyset. Fra å drive operasjoner i Irak, Afghanistan og Syria med «live feed» fra droner på hovedkvarteret ser man nå igjen behovet for å gi avdelingene mer autonomi ved behov og høyere grad av desentralisert ledelse via sjefens intensjon. «Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity.» (Patton)[12] Når egne hovedkvarter blir nøytralisert eller er i

10 USAF F-15 trente på å deployere ut fra Lakenheath til spredte baser for å øke overlevelse ved en eventuell konflikt med for eksempel Russland. https://warisboring.com/u-s-air-force-commandos-practice-refueling-rearming-f-15s/

11 https://sputniknews.com/russia/201608071044027427-russia-laser-weapons/

12 https://www.realcleardefense.com/articles/2016/09/02/the_problem_of_mission_command_110008.html

ferd med å flytte til alternativt hovedkvarter, er det avgjørende at avdelingene ikke blir pasifisert ved at de sitter og venter på ordrer. På Luftmaktseminaret i fjor kom Major Morten Hanche (første norske testpilot på F-35) inn på behovet for å tenke høyere grad av autonomi og delegering av myndighet til pilotene under operasjoner med F-35.[13] Ett av hans utsagn var: «Uten større grad av delegering vil vi neppe utnytte F-35 fullt ut.»[14]

Autonome operasjoner er imidlertid ikke noe nytt for Luftforsvaret. Da jeg startet å fly F-16 i 1996, var det fremdeles en del av operasjonskonseptet. Dersom man mistet kommunikasjon med hovedkvarteret, skulle man iverksette prosedyrer som lot avdelingene fortsette å slåss i henhold til sjefens intensjon. Man kunne scrambles til forhåndsplanlagte områder og lete på egen hånd etter fiendtlige fly og om nødvendig bekjempe disse. Det som er nytt, er at vi har en hel generasjon av piloter og offiserer som ikke har trent på dette eller hatt det som en del av sitt planverk på over tjue år. Men det er allikevel ett stort problem med vektleggingen av autonome operasjoner akkurat nå når vi diskuterer MDB. Vi har fått F-35 med sensorer som gir oss en enorm styrkning i situasjonsoversikten til et nivå hvor F-35-miljøet uttaler at de ikke tror de andre instansene i K2-kjeden vil klare å lede flyene på en optimal måte. Kombinerer du dette med at store deler av Luftforsvaret ikke har innsyn i F-35s kapasiteter grunnet sikkerhetsklarering, inviterer ikke det til diskusjoner med andre grener i Luftforsvaret og Forsvaret om hvordan man skal drive «multi-domain» kommando og kontroll. Hvis det er slik at det i MDB er samhandling og synergier på tvers av domenene som er løsningen på fremtidens krigføring, kan vi ikke ha Forsvarets F-35 flygende rundt på egen hånd uten å kommunisere med de andre forsvarsgrenene og hovedkvarterene sømløst ved behov.

Det som derimot bør være målsetningen i et MDB-perspektiv, er en utdyping av setningen til Hanche fra i fjor: **«Uten større grad av deling (av informasjon) som F-35 kan skaffe, vil vi neppe utnytte F-35 fullt ut!»** For å illustrere poenget: Under en øvelse i fjor sendte en amerikansk F-35 måldata om en måldrone fra egne sensorer via «Multifunction Advanced Data Link» (MADL) til en fregatt, som beskjøt målet med et langtrekkende luftvern, «Standardmissil 6» (SM-6).[15] MADL er en «stealthy» bredbånd-datalink som er vesentlig vanskeligere å detektere enn L-16, som per i dag er standard linksystem hos NATOs styrker. Et slik lavsignatur linksystem er altså helt i tråd

13 F-35 i luft-til-luft-rollen i «Evolution to a 5th Generation Air Force – Norway's Shield and Sword» s. 60.
14 Ibid s. 62.
15 https://www.raytheon.com/news/feature/sm-6_first_of_a_kind.html

med målet om å holde den elektromagnetiske signaturen på våre enheter og hovedkvarter nede. Kan det være fornuftig at data om en eventuell fiendtlig artilleribeskytning i Finnmark som sensorene på F-35 detekterer, blir gitt til en hæravdeling med langtrekkende Joint Strike Missile (JSM) på lasteplanet? Eller at målkoordinatene kan sendes til en amerikansk ubåt i Nordsjøen lastet med langtrekkende Tomahawk-missiler? Vi retter for tiden svært mye oppmerksomhet på hvordan vi skal få allierte avdelinger til landet raskt nok i en krisesituasjon. Men kan man tenke seg at man kan få beskutt fiendtlige mål i Finnmark ved hjelp av allierte langtrekkende presisjonsvåpen enda raskere? At norske F-35 bidrar til å produsere sensorinformasjon, deler situasjonsoversikten med hovedkvarter i Norge og NATO slik at FOH kan autorisere avfyring av amerikanske eller britiske kryssermissil? Det gikk 10 år fra F-16 fikk L-16 i 2003 til CRC-ene fikk L-16 og kunne sende luftbilde til flyene. La oss håpe det ikke går 10 år før NAOC, luftvernet, brigaden og fregattene får MADL.

US Navy og den nye norske luftmaktdoktrinen tar tak i problematikken med vektleggingen av autonomi ved å introdusere henholdsvis begrepene **«Flexive Command»** og **«sentralisert ledelse, *tilpasset* utførelse»**. Autonome operasjoner er lite praktisert i de siste krigene Vesten har vært involvert i, og det er flere grunner til det. En av dem er en reell frykt for at undergitte begår feil. Dette er en helt vanlig erfaring også internt i vårt eget kampflymiljø. Det er for øvrig en betraktning at vi i kampflymiljøet utad tenderer til å beskrive oss selv som en unison gruppe som mener og handler helt likt og ofte vet best, mens vi internt bruker timevis hver dag på å debriefe flyturer hvor vi slett ikke har oppført oss som en samlet enhet, men heller opplever å ha tatt ulike beslutninger gitt de samme inngangsverdiene! Autonome operasjoner kan altså ikke være primærløsningen i en eventuell fremtidig høyintensitetskonflikt, men må kun unntaksvis nyttes for å unngå at avdelinger blir passive ved kommunikasjonssvikt! Hvorfor er det viktig å poengtere at en fleksibel K2 må være målet? Jeg tror man ved å tilstrebe sentralisert ledelse vil gi et ekstra skyv til å utvikle redundans i kommunikasjonsstrukturen og en styrket forståelse for at man både fra ledelsen og undergittes side må prioritere å få gjenopprettet kommunikasjon så raskt som mulig etter at den er brutt. Man skal ikke bli paralysert ved at man ikke har prosedyrer for å operere autonomt, men avdelingene skal heller ikke forbli autonome!

Ser vi på hva USAF tenker om sin luftkommando og -kontroll, ser vi at de nå oppretter egne Air Operations Centers (AOC), som inkluderer space og cyber i hovedkvarteret i større grad. Videre har de nå skilt ut den offensive angrepsdelen av cyber fra e-tjenesten sin fordi e-tjenesten og operasjonene innimellom kan ha grunnleggende interesseforskjeller. Mens e-tjenesten ønsker å holde

sine operasjoner skjulte, kan operasjonsplanleggere ønske å ødelegge eller forstyrre fiendens operasjoner via cyber. NATO har også utvidet sin tilnærming til cyber ved å opprette et organ som i første omgang prøver å samordne nasjonale offensive ressurser utover etterretningsoperasjoner. Luftforsvaret er nok den forsvarsgrenen som er mest avhengig av cyberinfrastruktur, linker og kommunikasjon på lang avstand. Videre er satellitter avgjørende når det gjelder Positioning, Navigation and Timing (PNT), og ISR-satellitter bidrar til targetinginformasjon til luftstyrkenes presisjonsstyrte våpen. Norge bør også opprette egne enheter på FOH og NAOC som er i stand til å bedrive offensive cyberoperasjoner.

Hvordan får vi testet og synliggjort vår reelle reaksjonsevne, kampevne og utholdenhet? Brigade Nord har de siste årene ofte kjørt «Snap Exercises» til Finnmark og Troms. Når var det sist vi gjorde det i Luftforsvaret utover QRA og HLB? I 2006 ble det sist kjørt en nasjonal evaluering i kampflymiljøet på linje med det gamle evaluerings-regimet i NATO (Opeval). Siste NATO Opeval for kampflyvåpenet var i 2002. Deretter ble det vurdert som for dyrt, og man så heller ikke behovet. Etter 2014 er det nå igjen mulig å argumentere for at man bør la andre NATO-land se oss i kortene og uten varsel komme og teste vår beredskap, kampevne og utholdenhet. Og kanskje bør man ikke bare teste én og én avdeling slik praksis var tidligere, men faktisk utfordre hele Forsvaret til å teste flere avdelinger i Multi-Domain Battle. En pekepinn på tilstanden får vi i år gjennom øvelsen Trident Juncture. Vi bør bruke anledningen godt og ærlig notere oss utfordringene. Vi har allerede jobbet med øvelsen i månedsvis. Det burde egentlig være venstrehåndsarbeid for et land som er så avhengig av NATO-alliansens bidrag, å få kun 40 000 soldater og 150 fly hit. Det kommer til å koste penger, men spørsmålet er heller om vi har råd til å la være!

Konklusjon

Da gjenstår å gjenta konklusjonene jeg nevnte i starten av foredraget:

1 Luftforsvaret må utvikle et system av systemer for beredskap, kampevne og utholdenhet. Det finnes ikke en «Silver Bullet» som enkelt og billig løser alle disse utfordringene!
2 Luftforsvaret må ta ansvar for å utvikle «Multi Domain» kommando og kontroll med de øvrige forsvarsgrenene og ikke fokusere for mye på autonome operasjoner med F-35! Vi må altså lede helhetlig når vi kan, men kunne operere autonomt når vi må!

Referanser

Forsvarets stabsskole (2014). *Forsvarets Fellesoperative Doktrine*. Oslo: Forsvarsstaben.

Hanche, M. (2017). F-35 i luft-til-luft-rollen. I Larssen A. K. *Evolution to a 5th Generation Air Force – Norway's Shield and Sword?* (s. 57–64) Trondheim. Luftkrigsskolen

Søreide, I.E. (2016). En ny langtidsplan for forsvarssektoren – vårt utgangspunkt og våre valg. Foredrag på Oslo Militære Samfund, 12.01.2016 Hentet fra https://www.regjeringen.no/

Søreide, I.E. (2016. 6. okt.) hentet fra https://www.facebook.com/Forsvarsdep/videos/1478868418806196/

https://en.wikipedia.org/wiki/Fifth-generation_jet_fighter#Critics_and_alternative_definitions

https://www.oslomilsamfund.no/foredrag-forsvarssjefens-arlige-statusoppdatering-gjennomforingsevne-og-modernisering

https://www.vg.no/nyheter/innenriks/i/L01KXJ/nye-tall-norge-bruker-lavere-andel-p%C3%A5-forsvar-i-strid-med-nat-os-m%C3%A5l

https://warisboring.com/u-s-air-force-commandos-practice-refueling-rearming-f-15s/

https://www.raytheon.com/news/feature/sm-6_first_of_a_kind.html

https://www.realcleardefense.com/articles/2016/09/02/the_problem_of_mission_command_110008.htm

https://sputniknews.com/russia/201608071044027427-russia-laser-weapons/

En ny tid

av Espen Barth Eide

Jeg vil begynne med å si at jeg er enig med hovedbudskapet på dette seminaret – multi-domain må være mer enn joint, noe mer enn felles. Det dreier seg om å forstå hvordan moderne konflikt, krigføring og operasjoner foregår på tvers av gamle skillelinjer og på måter som vi aldri har opplevd tidligere. Slike konflikter kan være enda mer intense, endre seg raskere og ha enda høyere behov for umiddelbar situasjonsforståelse enn mer «tradisjonelle» konflikter. Dette går etter min mening langt ut over det kinetiske spektrum og påvirker blant annet politiske beslutningsprosesser og sivil infrastruktur.

Multi-domain og nye geostrategiske trender

Selv har jeg hatt gleden av å fra politisk hold lede arbeidet knyttet til anskaffelsen av F-35. Til den beslutningen ønsker jeg å knytte to refleksjoner, som jeg tror dere her i salen kjenner til, men som likevel er viktig å slå fast da refleksjonene er direkte knyttet til tematikken. Først vil jeg understreke at jeg håper dere i lyseblått liker flyene, for de koster noen kroner. De er for øvrig ikke kjøpt bare til dere. Selv om vi håper at dere passer pent på dem, er det nemlig en anskaffelse til hele Forsvaret. En helt sentral del av beslutningen om både å kjøpe nye kampfly og å stille de ekstreme kravspesifikasjonene som vi gjorde i samarbeid med Forsvaret, Luftforsvaret og forsvarssjefen, hadde å gjøre med nettopp Multi-Domain. Vi la stor vekt på flyets evne til å være en integrert del av et moderne og fremtidsrettet luftforsvar. Alle kandidatene vi sto igjen med, kunne jo både fly og levere våpen uten problem, og overoppfylte dette minimumskravet. Hadde vi sett for oss at våre fremtidige operasjoner ville være like dem vi opplevde i Bosnia, Kosovo og Afghanistan eller lignende scenarioer, kunne vi uten videre ha kjøpt hvilken som helst av de flymaskinene vi hadde til vurdering. Alle ville ha levert. Men allerede da beslutningen om å kjøpe kampflyene ble tatt i 2008, hadde vi erkjent at vi ikke lenger kan forvente at fremtidige kriger og konflikter bare vil være mellom oss som teknologisk overlegen alliert mot lavteknologiske aktører. Vi måtte ta høyde for at vi igjen kunne møte motstandere som ville vise seg teknologisk likeverdige med oss.

Dette var Norge tidlig ute med å si. Samme år som vi fattet beslutningen om

å kjøpe F-35, skjedde det to andre ting, henholdsvis én hendelse i Norge og én i sammenheng med NATO. Disse hendelsene illustrerer at vi så dette komme. Den ene er at vi la frem en langtidsplan, en av de to jeg har hatt ansvar for. I det sikkerhetspolitiske kapitlet beskrev vi at krig i Europa ikke kan utelukkes – det er ikke kun noe som «hører historien til». Væpnet konflikt mellom suverene stater i Europa er mulig, i vår tid også, påpekte vi. Det høres kanskje ut som en selvfølgelighet nå om dagen, men samme våren som vi la frem denne langtidsplanen, diskuterte politikerne i Storbritannia – av alle land – et White Paper som hevdet det stikk motsatte. Altså, at krig mellom stater i Europa hører hjemme i historiebøkene, og at vi må slutte med de gamle tenkemåtene. Fremtiden, mente de, var varianter av det britiske styrker den gang opplevde i Helmand i Afghanistan.

Dette var en åpen uenighet mellom Norge og en del andre vestlige allierte, mens mange av våre nye allierte i Øst-Europa var helt enige med oss. (Polen og baltiske land som selvsagt hadde meldt seg inn i NATO nettopp på grunn av artikkel 5, ble svært overrasket over at de straks etter at de hadde blitt ønsket velkommen til alliansen, ble spurt om når de kunne sende styrker til Balkan eller Afghanistan.) Høsten samme år la vi frem et dokument på et forsvarsministermøte, som vi kalte *Nærområdeinitiativet*. Det var et politisk innspill der vi fremholdt at alliansen igjen må fokusere på artikkel 5. Vi var på ingen måte motstandere av det som het «non-article 5», men vårt argument var at vi ikke kan ha en allianse som er opprettet for å ivareta *Area* og artikkel 5, men som til slutt bare opererer *out-of-area* og *non-article 5*. NATO kunne ikke bare ende opp som negasjonen av sitt eget formål, mente vi.

Det bidro til å skape en trend som nå har blitt helt normalisert. Da NATOs generalsekretær Jens Stoltenberg, som for øvrig var min regjeringssjef da vi besluttet å kjøpe F-35, kom på offisielt besøk til Norge, slo han fast at NATO nå har «vendt hjem». Øvelsen *Trident Juncture 2018* illustrerer vel dette bedre enn noe. Misforstå meg rett: Det betyr ikke at NATO aldri vil engasjere seg i oppdrag utenfor området eller artikkel 5, men det betyr at vi igjen fokuserer på at vi først og fremst er en militær forsikringspolise mot det verst tenkelige scenarioet – en storskala krig eller sikkerhetspolitisk krise med avanserte aktører i det symmetriske feltet. Under den kalde krigen var det én ting vi var opptatt av, og det var konflikten mellom øst og vest. Da tenkte vi «symmetrisk». Deretter falt Berlinmuren, og Sovjetunionen la ned seg selv, Warszawapakten ble oppløst, og mange var våre potensielle motstandere ble våre allierte. Plutselig var vi inne i en tid hvor vi ikke lenger fryktet *sterke*, men snarere *svake* stater og det kaoset og vakuumet som oppstår når stater slutter å virke. Eksempler er Balkan, Jugoslavia, Afghanistan, Irak og Libya. Meget raskt flyttet vi blikket fra

symmetri til asymmetri. Den tiden vi lever i nå, er dobbelt så komplisert. Dette skyldes at vi står overfor både symmetriske og asymmetriske utfordringer samtidig. Vi kan ikke slutte å bekymre oss for kaosbeltet sør og øst for Europa, som ikke blir borte. Samtidig må vi ta hensyn til at vi potensielt står overfor aktører som kanskje ikke er like store som oss i volum og økonomi, men som har investert i nytenkning for å oppnå relativ overlegenhet på visse felt, som da kan såre oss. Norge og noen andre land så disse trendene komme. Det henger altså sammen med kjøpet av F-35, som er et fly man kjøper fordi man tror, i hvert fall i teorien, at man kan trenge det mot en avansert motstander, og fordi man skjønner at man må ha integrerte, helhetlige systemer. Ellers ville vi heller ha spart penger og kjøpt noe som er billigere og leverer varene likevel, med tanke på utfordringene man så for seg rundt år 2000. Strategisk konkurranse er tilbake.

Den fjerde industrielle revolusjon

Vi lever i en tid med omfattende teknologiske endringer, også kalt den fjerde industrielle revolusjon. Jeg jobbet noen år i World Economic Forum, hvor begrepet den fjerde industrielle revolusjon oppsto. Ideen er at mange teknologiske utviklingstrekk som hver for seg er grensesprengende, for eksempel innen biomedisin, stordata, kunstig intelligens, nye materialer, nye produksjonsformer og nye former for kommunikasjon, ikke bare utvikler seg innen hver sin nisje, men kobles sammen på måter vi bare så vidt har begynt å forstå. Det er en generell utfordring for land, næringsliv og arbeidstakere verden over.

Men dette betyr også mye for feltet Multi-Domain. Om tiden vi går i møte, kan vi med stor sikkerhet si at både venner og fiender kommer til å utvikle helautonome våpensystemer med kunstig intelligens som har tilgang til enorme mengder data. (Disse systemene er ikke nødvendigvis begrenset til fysiske apparater som droner, de kan også være digitale.) Systemene vil da kunne være i stand til å få oppdrag fra mennesker og deretter løse dem selvstendig ved hjelp av data de har tilgjengelig. Ved å benytte seg av den enorme datamengden som vi mennesker etterlater oss overalt, kan systemene lete etter ting, systemer, personer og organisasjoner og slå til med en eller annen form for skade som enten er kinetisk eller kybernetisk. Dette er ikke lenger science fiction, det har skjedd og skjer nå. Dette er en dramatisk utfordring som gjør at vi må tenke militærteoretisk nytt. Siden steinalderen og klubbenes tid og til dagens missiler har man i det minste hatt litt varslingstid ved hjelp av framsynthet, etterretning og sensorer – enten måneder fra man ser en fremmed hær

samle seg på andre siden av grensen, eller minutter før man ser innkommende missiler eller fly. I cyberdomenet er man derimot svært heldig hvis man vet at man blir angrepet nå. Normalt vet man at man ble angrepet i går, for en måned siden eller for flere år siden. I mange tilfeller har vi allerede blitt angrepet ved at det ligger sovende celler som venter på å bli aktivert. Dette gjelder ikke nødvendigvis i Forsvarets datasystemer. Det kan like gjerne være sovende celler som ligger klare til bruk i Hafslunds strømstyringssystemer eller Bergens vannforsyningssystem.

Hvis vi havner i en sikkerhetskonflikt med en annen stat, tror jeg det usannsynlig at konflikten begynner med stridsvogner og fly som kommer inn over grensen. Lenge før det skjer, har vi blitt forvirret og utsatt for informasjonsoperasjoner. Ikke bare operasjoner som omfatter konkrete, fysiske forsøk som å stjele, ødelegge eller manipulere vår egen informasjon på den måten at våre systemer lurer oss selv, det vil også være informasjonsoperasjoner mot befolkningen og på sosiale medier. Et betydelig moment å ta med seg er at vi lever i en tid hvor følgende har gjort seg gjeldende: Da jeg var ung, la man til grunn at det man fikk vite gjennom tradisjonelle nyheter, hadde høyere sannsynlighet for å være sant enn det man bare plukket opp andre steder. Nå skjer det derimot en utglidning hvor mange mennesker uttrykker mistro til disse tradisjonelle medier og henter informasjonen sin fra Facebook, Twitter eller andre alternative kilder. Vi vet at aktører utnytter dette for å skape usikkerhet, uro, forvirring, bekymring og tvil rundt det myndighetene sier. Disse tingene ville ha forekommet før man befant seg i en kinetisk situasjon.

Totalforsvar 2.0

Grunnen til at jeg sier dette, er at Multi-Domain definitivt omfatter luft, sjø, land, space og Forsvarets cyberkapasiteter. Det sistnevnte trenger vi at dere får til så godt dere overhodet kan. Men det er ikke bare Forsvarets cyberkapasiteter som er relevant, men også Bergens vannverk, Hafslunds strømsystemer, Telenors telekommunikasjon og regjeringens evne til å ta beslutninger i komplekse situasjoner. Vi må huske på at den gammeldagse krigen, slik vi som regel har tegnet den, ofte har en avklart begynnelse og slutt. Bare tenk på andre verdenskrig: vi vet nøyaktig når den startet for Norge. Den startet da Oberst Eriksen åpnet ild mot Blücher som var på vei inn fjorden, og sluttet på formiddagen 8. mai da hjemmestyrkene overtok kommandoen på Akershus festning. Først fred, deretter krig i fem år, og så ble det fred igjen da tyskerne kapitulerte og reiste hjem. Og selv om det var en verdenskrig, var det områder som ikke var direkte involvert, for eksempel Sverige og Sveits. Slike land var ikke involvert

fordi man faktisk respekterte de definerte fysiske grensene for hvor krigen ble utkjempet. Med andre ord: vi kan svare presist både på *når* og *hvor* andre verdenskrig fant sted.

I dag vet vi derimot ikke når krigen starter, eller om den i det hele tatt har startet og i så fall når den slutter. Når begynte krigen mot IS? Det er åpent for tolkning. Er den over? Vel, den er ikke så intens som den var, men borte? Tja. Hvor skjer den? I Raqqa, ja, men også i Paris og Brussel, og mange andre steder. Med andre ord: De markørene som gjorde det mulig å si at dette er fred og dette er krig, er i ferd med å forsvinne. Det er synd at tiden da vi kunne vite at det var krig eller ikke, er forbi. Det er kanskje ikke krig direkte, men vi er hele tiden med i en strategisk konkurranse. Poenget med å understreke dette er at jeg som politiker og tidligere forsvarsminister anser at Multi-Domain innebærer at vi må tenke *utenfor* Forsvaret og forstå den store samfunnsmessige konteksten. Dette har også å gjøre med totalforsvaret, som vi trenger versjon 2.0 av. Igjen vender jeg tilbake til tiden da jeg var ung, da var totalforsvaret det sivile samfunnets evne til å støtte Forsvaret i krig. Hvis man hadde firehjulsdrevet bil, sto den på en liste slik at den kunne rekvireres. Sjøheimevernet besto av fiskebåter med maskingeværfeste. I tilfelle krig festet man en 12,7 mm mitraljøse på fiskebåten, som hadde dyktig mannskap som kjente kysten, og som kunne drive med nærforsvar og observasjon. Dette var totalforsvaret i gamle dager. Nå er derimot spørsmålet om det er de militære eller de sivile domenene som blir angrepet, langt mer komplisert. Det krever at diskusjonen som Luftforsvaret har rundt Multi-Domain, ikke stopper ved den siste forsvarsgrenen. Man må løfte den ut av det militære feltet.

Sårbarhet og sivil-militær dialog

En venn av meg, Rod Beckstrom, er tidligere leder av Internet Corporation for Assigned Names and Numbers (ICANN). Det er ikke alle som vet hva ICANN er, men det bør dere vite – de sørger for at internett faktisk virker, som er et sentralt poeng for oss om dagen. Han har lansert opp en meget enkel «lov», som han kaller Beckstroms lov, med tre punkter: «1. Everything that is connected is vulnerable. 2. Everything is connected. 3. Everything is vulnerable.»

Ser man på det fantastiske samspillet mellom fregatter, F-35, sensorer på hærens systemer og koblinger til kommandosystemene, ser man at vi har skapt meget avanserte systemer som sammen gir mulighet for å utøve kinetisk effekt på måter vi tidligere bare kunne drømme om. Samtidig møter vi to utfordringer: Første punkt er at vi gjerne vil ha informasjonen som følger av dette samspillet, og vi vil gjerne at det virker, også i de mest kritiske situasjonene, altså at

den ikke blir forstyrret. Vi ønsker med andre ord å skjerme systemenes integritet. Det andre er at vi gjerne vil ha informasjonen selv, da det er fint at det er vi, og ikke fienden, som har det svært sofistikerte bildet som dette samspillet har skapt. Å forstå betydningen av sårbarhet vil bli ekstremt viktig i fremtiden. Jeg vil ta dette videre med et eksempel: Å slå ut ett enkelt vannkraftverk i Norge skaper ikke spesielt store problemer, da det fort vil kompenseres for gjennom det svært avanserte samspillet i energinettet. Det en angriper må gjøre, er å ødelegge de systemene som gjør at dette høyteknologiske, komplekse samspillet virker. Dette gjelder også alle andre lignende områder, slik som telekom – det mest logiske «entry point» hvis man skal angripe Norge, er altså de komplekse systemene som gjør at samspillet fungerer. Hva gjelder forsvar av cyberspace, er det med andre ord ikke nødvendigvis slik at det er fysisk vakthold utenfor trafostasjonen som er viktigst for Forsvaret.

Vi står overfor en ny teknologisk æra. Et viktig begrep er «weaponization», som betyr at man konverterer eksisterende sivil teknologi til våpen. Et klassisk eksempel er da 9/11-terroristenes konverterte sivile fly til svært effektive missiler som ingen kunne forberede seg på, fordi man ikke kunne vite før det var alt for sent at flyet i praksis var blitt et missil styrt av selvmordsbombere. Et militært missil på vei inn fra utlandet kan skytes ned fordi man forstår hensikten med missilet, det gjør man ikke på samme måte med morgenflyet fra Boston. Dette er et eksempel på innovativ bruk av sivil teknologi.

Når tradisjonelle våpenprodusenter lager våpen, vet de jo godt at de må passe på hvem som får tak i våpenteknologien, og hvilke nasjonale og internasjonale regler de må følge. Dette gjelder ikke nødvendigvis i sivil sektor – de som lager produkter ment til sivil bruk, har kanskje ingen tanke om eller forståelse for at produktene også kan brukes til helt andre formål. Da bygger de heller ikke inn sikkerhetssystemer for å hindre «weaponization» av produktene, og vi har i dag ikke mekanismer for å hindre det. Denne utfordringen må også inkluderes i tenkningen rundt Multi-Domain.

Det er ikke slik at dette ikke har blitt tenkt på, men vi som sitter på Stortinget, må tenke mer på disse tingene. Vi står altså overfor noen utfordringer som gjør at vi må lære oss å ha en sivil-militær dialog om hvordan vi møter disse, som er helt annerledes enn før.

About the Authors

Major General **Tonje Skinnarland** started her military career in 1987 at the RNoAF NCO School. As a Brigadier, she was the acting Chief of the Norwegian Air Force from 2016. In February 2017, she was appointed Chief of the Norwegian Air Force.

Frank Bakke-Jensen has been a Member of Parliament since 2009, and was appointed Minister of Defence in October 2017.

Carl Bildt has served as both Prime Minister and Foreign Minister of Sweden. Subsequently, he served in international functions with the EU and the UN, primarily related to the conflicts in the Balkans as Special Envoy of UN Secretary General Kofi Annan. He serves as one of the Senior Advisors to the Wallenberg Foundations in Sweden and is on the Board of Trustees of the RAND Corporation in the US.

Øystein Tunsjø is a professor at the Norwegian Institute for Defence Studies. Tunsjø holds a PhD in International Relations from the University of Wales, Aberystwyth, a Cand. Philol. in History from the University of Oslo, an MSc from the London School of Economics, and an MA from Griffith University, Australia. Tunsjø was a visiting Fulbright scholar at the Fairbank Center for Chinese Studies, Harvard University, during spring term of 2010.

Pasi Eronen recently completed a major Russia project for the DC-based think tank Foundation for Defense of Democracies (FDD). He is a featured expert on Atlantic Council's DisinfoPortal. His professional career includes working for the Finnish defense establishment and governmental organizations dedicated to comprehensive security and countering hybrid threats. He has also served in crisis management missions both with the EU and NATO. Eronen earned a master's degree in Security Studies from Georgetown University, USA, and a master's degree in Computer Science from the University of Joensuu, Finland.

Geir Lundestad is a Norwegian historian who, until 2014 served as the Director of the Norwegian Nobel Institute. He studied history at University of Oslo and University of Tromsø, graduating in 1970 with a cand.philol. degree, and in 1976 with a doctorate respectively. He has spent several years in the United States as a research fellow, at Harvard University, and at the Woodrow Wilson Center in Washington. He was an adjunct professor of international history at the University of Oslo from 1991 to 2014.

Brigadier General **David W. Hicks** is the Director of Strategy, Concepts, and Assessments, Deputy Chief of Staff for Strategic Plans and Requirements, Headquarters U.S. Air Force. He holds a BA in Engineering Mechanics and an MA in Systems Engineering from Air Force Institute of Technology, Wright-Patterson AFB, Ohio.

General **Frank Gorenc** was the Commander of U.S. Air Forces in Europe, U.S. Air Forces Africa, NATO Allied Air Command, and Director of Joint Air Power Competence Centre, Kalkar, Germany. He was the air component for European Command, Africa Command and NATO. He holds a BA in civil engineering, an MA in Aeronautical Science, and an MA in national security strategy. As a command pilot, he flew over 4,900 hours in the F-15C, T-38A, MQ-1B, UH-1N, and C-21. He retired in October 2016 and is now a consultant, public speaker and a board director for several companies.

Colonel **Michael D. Runey** is assigned as the Division Chief of the Joint and Army Concept Development for the Army Capabilities Center. He has served as an Instructor of Military History at the United States Military Academy in West Point, New York. Prior to his recent assignment, COL Runey served as the Director of the Security Force Assistance Center for NATO Headquarters in Kabul, Afghanistan.

Olav Lysne is a professor of Communication Systems at the University of Oslo, founder of the Center for Resilient Networks and Applications at Simula Research Laboratory, and director of Simula Metropolitan. Lysne was the leader of National Commission for Digital Vulnerability formed by the Norwegian Government (Lysne I-utvalget). Lysne was the leader of a National Commission that assessed whether the Norwegian Secret Service (Etterretningstjenesten) should be allowed to do lawful interception of Internet traffic crossing the national borders of Norway (Lysne II-utvalget).

Cadet **Eva Johanne Merkesdal** is a Norwegian Air Force Academy Cadet in her second year. She has work experience from maintaining helicopters at 339 Sqn at Bardufoss.

Dr. **Lior Tabansky** is a scholar of cyber power at Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center. Lior's doctoral dissertation in Political Science uncovered failed peacetime defense adaptation, that exposes developed societies to destructive cyberattacks on strategic homeland targets by foreign states. Leveraging 15 years of IT-pro work and business experience in formulating cyber strategies, his current research interests are National Innovation Systems and capacity building; defense adaptation; Hostile Influence Operations online. http://www.tau.ac.il/~liort/

Major General **Inge Kampenes** is the Commanding Officer of the Norwegian Armed Forces Cyber Defence. His previous position was Director of Long-term Planning in the Air Force Staff. He also led the work on CHOD's Strategic Defence Review 2015. He has operational fighter pilot experience from all squadron levels, and has flown both F-5 and F-16. He holds a PhD in Course Complexity Leadership from the University of Bodø.

Lieutenant Colonel **Harald Høiback** was at the time of the seminar senior lecturer at the Defence Staff College, but is now Deputy Commander at The Norwegian Armed Forces museums. In his military career, he has done service in Finnmark, Afghanistan, and in the Norwegian Department of Defence. He holds an MA in history from the University of Glasgow and a PhD in philosophy from the University of OsIo. He has written and contributed to a number of books, the most famous being "Understanding Military Doctrine: A Multidisciplinary Approach' (2013).

Major General **Lars Christian Aamodt** is Deputy Commander/Chief of Staff at Norwegian Joint Headquarters. He started as an Officer Candidate in the Navy but switched to the RNoAf Pilot Training programme. He is a fighter pilot and has flown F-16.

The Air Staff/Vice Chief of the Norwegian Air Force is Brigadier General **Aage Lyder Longva**. He started his military career in the RnoAf Pilot Training Programme in 1984. He is a Fighter Pilot and has flown both F-5 and F-16.

Colonel **Morten Jensen** is the Artillery Inspector at the Norwegian Land Warfare Centre. His previous position was Commanding Officer Artillery Battalion Brigade North. He has also commanded the Norwegian Provincial Reconstruction Team in Maymaneh, Afghanistan.

Rear Admiral **Nils Andreas Stensønes** is Chief of the Norwegian Navy. He graduated from the Royal Norwegian Naval Academy in 1987. His most recent assignment was Deputy Chief of Staff for Operations at the Norwegian Joint Headquarters.

Colonel **Stig Eivind Nilsson** is the Head of the Norwegian Ministry of Defence Space Programme. He started his career at the RNoAF Pilot Training Programme in 1984. He is an F-16 fighter pilot by profession.

Major **Jens Gunnar Dragsnes** holds a military career as a fighter pilot and officers' trainer both at the Air Force Academy and Command and Staff College. He has served as XO for 338 Sqn at Ørland and as Squadron Commander for 332 Sqn in Bodø. He flew in Operation Allied Force and Operation Enduring Freedom. He is now an instructor in Air Power at the Air Force Academy.

Espen Barth Eide is a Member of the Norwegian Parliament for 2017-2020, representing the Labour Party. In 2014, Espen Barth Eide was appointed United Nations Special Adviser on Cyprus, and held this position until 2017. He served as Norway's Minister of Defence in Stoltenberg's Second Cabinet from November 2011 to September 2012, and subsequently as Minister of Foreign Affairs until October 2013.