

Informasjonsoperasjoner

Foredrag ved Oslo militære samfunn, 13 mars 2000

Kommandørkaptein Inge Tjøstheim, FSTS

1 Innledning

Hva er informasjonsoperasjoner? Er informasjonsoperasjoner og informasjonskrigføring det samme? Er informasjonsoperasjoner noe nytt som kjennetegner 1990-årenes og fremtiden fredsstøttende eller kriserespons operasjoner? Er informasjonsoperasjoner en annen betegnelse på kybernetisk krigføring eller *cyberwar* som amerikanerne sier?

Dette er noen av de spørsmål jeg skal forsøke å gi svar på i løpet av dette foredraget. Og la det med en gang være sagt: informasjonsoperasjoner er ikke noe nytt! For over to tusen år siden skrev den kinesiske militærfilosof Sun Tzu at de "som i gamle dager var ansett for å være dyktige til å føre krig, beseiret slike som var lette å beseire ... [de] beseirer den som allerede har tapt"¹. Hvordan kan vi så seire over noen som allerede har lidt nederlag? Jo, sier Sun Tzu, det kan vi ved først å bruke alle tilgjengelige midler og metoder for "å angripe fiendens planer"². Det viktigste virkemidlet den gang var bruk av allslags agenter for å innhente informasjon og plante desinformasjon. Hvis vi kan bruke uttrykket 'krig' på den epoke vi kalte 'den kalde krigen' og ser på hvilke virkemidler 'de stridende' blokker benyttet mot hverandre, er det tilsynelatende bare nyanse forskjeller mellom informasjonsoperasjoner og informasjonskrigføring, men informasjonsoperasjoner er et penere, mer sivilert uttrykk, på samme måte som informasjon er penere og mindre belastet enn propaganda.

Etter disse innledende betraktninger skal jeg nå først forsøke å definere informasjonsoperasjoner slik begrepet oppfattes i dag. Deretter skal jeg forsøke å gi en del historiske eksempler på denne moderne definisjonen for å vise at det tilsynelatende ikke er så mye nytt. Jeg sier 'tilsynelatende' fordi det faktisk er et helt avgjørende nytt aspekt ved denne type operasjoner som vi må forholde oss til i dag og i fremtiden. Jeg vil avslutte med å si noe om hva dette nye er og hvilke konsekvenser det har for Norge som en suveren stat og for Forsvaret som et sikkerhetspolitisk virkemiddel.

2 Definisjon av informasjonsoperasjoner

NATO har ennå ingen endelig godkjent definisjon på informasjonsoperasjoner, selv om det foreligger et utkast. Forsvarets fellesoperative doktriner, har en definisjon som er i overensstemmelse med NATOs. Den lyder som følger:

Tiltak iverksatt for å påvirke beslutningstakere til støtte for egne politiske og militære målsettinger. Tiltakene har til formål å påvirke andres informasjon, informasjonsbaserte prosesser, kommando- og kontrollsystemer (K2S), og kommando- og informasjonssystemer (KIS) mens vi utnytter og beskytter vår egen informasjon og våre egne K2-systemer og KI-systemer. Informasjonsoperasjoner utnytter grensesnittet mellom teknologiske nyvinninger og den mest kritiske faktor i ethvert aspekt ved krigføring - mennesket. Det finnes to kategorier av informasjonsoperasjoner: defensive InfoOps og offensive InfoOps, avhengig av hvilke tiltak som iverksettes.

Fra et militært perspektiv er det grunnleggende formålet med informasjonsoperasjoner å sikre tilgang på nødvendig informasjon og hindre en motstander tilsvarende. Denne informasjon skal brukes til å bygge opp og vedlikeholde en kunnskap om operasjonsområdet som er bedre enn motstanderens, for dermed å oppnå en informasjonsoverlegenhet eller -dominans, som igjen kan bidra til et økt tempo i vår og et svekket tempo i en motstanders handlingsløype.

Vi kan skille ut to nivåer eller typer av 'militære' informasjonsoperasjoner i denne prosess. Den først må håndtere informasjonsoperasjoner innenfor hele info- og infrastrukturen (sivile og militære sensorer, kommunikasjoner og nettverk) for å oppnå informasjonsoverlegenhet som grunnlag for planlegging forut for og under en militær operasjon. Den andre typen må under operasjonene sikre at land-, sjø- og luftoperasjonene kan koordinere innsats mot utvalgte mål. Den siste type forutsetter effektiv kommando og kontroll, og en koordinert bruk av de virkemidler vi har til kommando- og kontrollkrigføring³, herunder operasjonssikkerhet (OPSEC), fysisk og elektronisk villedning, psykologiske operasjoner (PSYOPS), elektronisk krigføring (EK) og midler til fysisk ødeleggelse. Før jeg gir noen historiske eksempler på bruk av denne type virkemidler, er det naturlig å si noe om strategiske informasjonsoperasjoner.

3 Strategiske informasjonsoperasjoner

Strategiske informasjonsoperasjoner har vært et viktig virkemiddel for å påvirke utfallet av militære konflikter og kriger gjennom hele det 20. århundre, men også i fredstid for å fremme nasjonale interesser.

Allerede dagen etter at Storbritannia erklærte Tyskland krig i august 1914, seilte det kongelige kabelskip *Telconia* ut i Nordsjøen og kuttet alle Tysklands fem kommunikasjonskabler til omverdenen. Etter den dag gikk det synet resten av verden hadde på krigen i økende grad gjennom en linse som var lokalisert i London. Det gjorde det mulig for britene å iverksette en effektiv strategisk informasjonskampanje som til slutt bidro til å få USA med i krigen på de alliertes side. Britene førte med andre ord en strategisk informasjonskrig mot Tyskland.⁴

Under annen verdenskrig hadde USA både et *Office of War Information* (OWI) og et *Office of Strategic Services* (OSS), forløperen til CIA, hvor det første var "ansvarlig for spredning av offisiell amerikansk propaganda som åpent springer fra amerikanske kilder" utenfor fiendens eller fiendtlig okkupert territorium og OSS for spredning av "sann eller falsk" propaganda som har sin opprinnelse "inne fra fiendtlig eller fiendtlig okkupert territorium".⁵

Av relevans for håndtering av fredsstøttende operasjoner, både for å få et bilde av hvilke kulturelle krefter vi står overfor og for å gjennomføre virkningsfulle informasjonsoperasjoner mot befolkningsgrupper, kan jeg nevne at under annen verdenskrig bruke amerikanerne mange sosialantropologer i arbeide som "psykologiske planleggere". Noen ble f eks brukt som rådgivere for radiostasjoner styrte av OSS og som hadde til formål å undergrave japansk propaganda i Burma og Thailand.⁶

Informasjonsoperasjoner er også et strategisk virkemiddel ved siden av trussel om bruk av militærmakt i fredstid. Som eksempel kan jeg nevne at Reagan administrasjonen i 1984 utga et *National Security Decision Directive 130*, med tittelen *US International Information Policy*, som skisserte en strategi for bruk av informasjon og informasjonsteknologi som et strategisk instrument for å forme grunnleggende politiske, økonomiske, militære og kulturelle krefter på langsiktig basis for å påvirke globalt atferden til regjeringer, internasjonale organisasjoner og samfunn til støtte for amerikansk sikkerhet⁷.

Også i forbindelse med konfliktene på Balkan i 1990-årene har strategiske informasjonsoperasjoner spilt en sentral rolle. Allerede i begynnelsen av 1993 var PR-krigen, ifølge David Owen, "et tydelig trekk ved krigen i Bosnia-Hercegovina. Dokumenter lagret i det amerikanske justisdepartementet viser at Kroatia betalte ... et PR firma i Washington, \$10.000 per måned pluss utgifter for å 'presentere et positivt bilde av Kroatia' for medlemmer i Kongressen, medlemmer av administrasjonen og nyhetsmediene." Også den bosniske regjering betalte for tjenester som omfattet "skrivning og plassering av redaksjonelle motinnlegg, gjeste skribenter og brev til redaktøren."⁸

Ejup Ganic, visepresident i Bosnia Hercegovina fra 1992, sa direkte til David Owen at han hadde et sentralt politisk mål, "nemlig å trekke US Army inn i Bosnia som krigførende for å beseire Serberne." For å få til dette mente han at alle mulig midler var tilatt. "For ham rettfærdiggjorde målet midlene. Han arrangerte den bosniske regjeringens propaganda og opererte på alle nivåer i USA - overfor Det hvite hus, Kongressen og på TV skjermene i

amerikanske hjem." Han var f eks imot demilitarisering av Sarajevo fordi det "ville fjerne det kraftigste våpen i hans propaganda arsenal for å trekke USA inn i konflikten."⁹

4 Kommando- og kontrollkrigføring

Selv om alle i dag er opptatt av begrepet informasjonsoperasjoner, har ikke dette erstattet kommando- og kontrollkrigføring. Sammenhengen mellom disse to begreper er meget innfløkt og det vil sannsynligvis bli stadig vanskeligere å skille mellom dem som følge av utviklingen innenfor informasjons- og kommunikasjonsteknologien.

Jeg skal i det følgende gi noen eksempler på aktiviteter som har vært og fremdeles er knyttet til kommando- og kontrollkrigføring.

4.1 Elektronisk krigføring og villedning

Straks det elektromagnetiske medium ble tatt i bruk til kommunikasjon (f eks telegraf) og til innhenting av informasjon (f eks radar), ble det viktig for de krigførende parter å beskytte egne systemer og angripe fiendens. Dermed oppsto EK som en egen krigføringsfunksjon.

Under det tyske angrepet på Frankrike i 1914 var radio den eneste kommunikasjon mellom de fremrykkende korps og hovedkvarterene. Radiomeldingene ble kodet og dekodet for at franskmennene ikke skulle forstå hva som ble sagt. Det å avlytte fiendens telegraf og radio er like gammel som systemene selv. For å hindre at de tyske korpssjefene kunne kommunisere med sine undergitte sjefer og danne seg et bilde av hvordan situasjonen utviklet seg, plasserte franskmennene en kraftig sender på toppen av Eiffeltårnet for å jamme de tyske radioforbindelsene.¹⁰ Å jamme en motstanders kommunikasjons- og sensorsystemer har siden vært et viktig element i elektronisk krigføring.

Under annen verdenskrig ble elektronisk krigføring stadig mer avansert og ble en viktig forutsetning for om militære operasjoner skulle lykkes eller ikke.

Hvis de allierte skulle oppnå en taktisk overraskelse D-dag måtte de radarstasjonene som vokter invasjonsområdet ødelegges helt eller delvis. Men for å skjule de alliertes fokus på Normandie, ble stasjoner i andre områder bombet enda mer intenst. Noen ble imidlertid med vilje ikke ødelagt - de skulle nemlig brukes for elektronisk villedning.

Under verdenskrigen testet og forbedret de allierte en rekke narretiltak som skulle tas i bruk på D-dagen. Alle involverte såkalte elektroniske motmidler (ECM), som var konstruert spesielt for å lure det tyske radarutstyret som var intakt.

En av disse oppfinnelsene var basert på det elektromagnetiske feltet som dipolen produserte, og som britene ga kodenavnet 'window', bedre kjent under den amerikanske betegnelsen *chaff*. Det besto av strimler av folie som kunne kastes i store mengder fra fly og skape en virkning på radarskjermen, ikke ulik en snøstorm på menneskets øye; det ble umulig å skjelne mellom objekter. Dette er et typisk eksempel på utnyttelse av en kritisk sårbarhet innenfor kommando og kontroll, og som er fremhevet i definisjonen på informasjonsoperasjoner, nemlig at "informasjonsoperasjoner utnytter grensesnittet mellom teknologiske nyvinninger og den mest kritiske faktor i ethvert aspekt ved krigføring - mennesket."

Britene utviklet også et annet våpen i elektronisk krigføring som tyskerne ikke hadde. Et britisk kvinnelig forsker hadde oppdaget at når dipoler ble droppet fra noen få fly på en bestemt måte, ga de ekkoer på radarskjermene som liknet det en stor luftstyrke ville ha gitt. Denne oppdagelse førte til utvikling av et apparat, betegnet *Moonshine*, som kunne installeres om bord i fly eller fartøyer. *Moonshine* mottok pulsene fra fiendens radar, forsterket og returnerte dem for å skape symptomer på radarskjermene som lignet dem frembragt av et stort antall skip eller fly som var under veis.¹¹ Dette er igjen et eksempel på manipulering av det kritiske grensesnittet mellom maskin eller teknologi og menneske, her representert ved radarskjermen, med alvorlige konsekvenser for fiendens kommando og kontroll.

Hvis det lyktes å forvirre og ødelegge disse tekniske nyvinningene som det tyske forsvaret var basert på, ville elektronikk bli bekreftet som en ny dimensjon i krigføringen, et våpen like

revolusjonerende som geværet, maskingeværet og stridsvognen. Dette er helt i overensstemmelse med det en av det 20. århundres største militærteoretikere, generalmajor John F C Fuller (1878-1964), skrev i 1960, at den industrielle revolusjon i 1940-årene gikk inn i sin tredje fase ved utviklingen av atomenergi og utviklingen av "elektronisk kontrollerte innretninger [...] Hensikten med denne siste er gradvis å innsette maskiner i stedet for menneskehjernen, på samme måte som Watts dampmaskin og Daimlers bensinmotor skulle innsettes i stedet for musklene til mennesker og dyr".¹²

4.2 Psykologiske operasjoner og spesialoperasjoner

Det er imidlertid ikke bare teknologi som står i fokus når vi taler om informasjonsoperasjoner og kommando- og kontrollkrigføring. Om Den amerikanske borgerkrigen sier den samme Fuller:

*Som de totale krigene i det tyvende århundre startet den etter flere år med voldsom propaganda, som lenge før krigen hadde utslettet alle former for moderasjon, og hadde hos de stridende parter vekket stamme-fanatisme primitive ånd.*¹³

Denne beskrivelse kunne like godt være myntet på det vi har sett under de forskjellige konfliktene på Balkan i 1990-årene. Dette viser at de psykologiske aspektene ved krigføring kan ha betydelige konsekvenser for hvordan væpnede konflikter føres og mulighetene for å løse dem når kamphandlingene er stanset. Denne erkjennelse er helt i overensstemmelse med Clausewitz som sier at i krig er hensikter basert på følelser mest fremtreden hos udannede folk, mens de som er basert på forstanden er mest fremtredende hos dannede folk. Men, sier han, "denne forskjellen ligger ikke i det å være udannet eller danned, men i de ledsagende omstendigheter, institusjoner, osv", og avslutter med å si: "Selv de mest dannede folk kan hate hverandre med brennende lidenskap."¹⁴ Fuller mener f eks at Churchills brennende hat til det tyske folk var et av motivene bak terrorbombingen av de tyske byene under annen verdenskrig og kravet om betingelsesløs kapitulasjon.

Robert A McClure, mannen som skapte spesialstyrkene i *US Army*, hadde under annen verdenskrig ansvaret for å bygge opp en informasjons og sensur seksjon (ICN) i Eisenhowers hovedkvarter forut for invasjonen av Nord-Afrika i 1942. I et brev fra 1943 skriver han følgende om seksjonens virksomheten:

*Vi opererer 12 kraftige radiostasjoner. Min stab for psykologisk krigføring – [som dekker] radio, flygeblad, signaler, [personell i] forreste linje, i okkuperte områder [...] – overstiger 700. I sensuren – tropper, brev og telegram, sivile brev, radio, presse, telegrammer, telefon for hele Nord- og Vest-Afrika, Sicilia, etc, over 400 personer og kontroll over 700 franskmenn. Publikumsrelasjoner [PR] – presse og korrespondenter – 150 korrespondenter [...] – en fullstendig 'kommando' på 1500 i en organisasjon som man aldri har forestilt seg i hæren.*¹⁵

Et resultat av de erfaringer som amerikanerne høstet under annen verdenskrig, fra avnazifiseringen av Tyskland etter krigen og fra Koreakrigen i begynnelsen av 1950-årene, var opprettelsen av det psykologiske krigføringssentret i Fort Bragg i mai 1952. Dette senter for ukonvensjonell krigføring hadde følgende tredelte oppdrag:

*Å gjennomføre individuell trening og kontrollere trening av enheter i psykologisk krigføring og operasjoner med spesialstyrker; å utvikle og teste doktriner, prosedyrer, taktikk og teknikker innenfor psykologiske operasjoner og spesialoperasjoner; å teste og evaluere utstyrt til bruk i psykologisk krigføring og spesialoperasjoner.*¹⁶

Britene hadde også sine organisasjoner for denne type virksomhet. Allerede i 1940 ble *Special Operations Executive* (SOE) dannet etter påtrykk fra Churchill. Den skulle utføre raids mot fiendtlig besatte områder med inntil 30-50 håndplukkede menn – blant annet flere raids mot norskekysten med støtte fra marinen og flyvåpnet. Et slikt raid mot Lofoten i februar 1941 var et

ledd i informasjonskrigen. Da ble en væpnet tysk tråler, *Krebs*, angrepet, kapteinen drept og kryptomateriell fjernet. Det gjorde det mulig for det topp hemmelige kryptoanalysestret i Bletchley Park nord for London å lese den tyske marinens signaltrafikk i februar og forskjellige dager fra 10 mars 1941.¹⁷

5 Informasjon, koder og kunnskap

Informasjonsoperasjoner kan helt generelt sies å være et uttrykk for enhver form for kamp om kontroll over informasjon. Hva er det så vi mener når vi snakker om 'informasjon'? Hvis jeg i dagligtalen spør deg om du har informasjon til meg, så mener jeg om du vet noe jeg ikke vet. For oss mennesker vil altså tilgang på informasjon gi oss kunnskap. Mangel på informasjon kan derimot frata oss muligheten for å handle fordi vi ikke har tilstrekkelig kunnskap eller fakta om en gitt situasjon. Det finnes også en tredje mulighet knyttet til informasjon og som jeg allerede har gitt noen eksempler på: Vi kan sørge for at en mottaker får feilaktig informasjon slik at han handler ut fra en innbilt kunnskap. Kunsten her er å gi mottakeren en informasjon han oppfatter som troverdig og som gjør at han handler slik som vi forventer. Desinformasjon, elektronisk og fysisk villedning har dette som målsetting.

Informasjon og kunnskap har alltid vært viktige parametre i konflikter og kriger, og derfor er heller ikke informasjonskrigføring et nytt fenomen. Det å beskytte informasjon mellom egne styrker ved å chifrere eller kode meldinger er like gammel som krigskunsten.

Fra oldtiden og frem til 1939 var det primært to metoder å kode meldinger på. Den ene metoden var alfabetforskyvning, f eks at A skulle skrives som D, B som E, osv. Denne metoden går i hvert fall tilbake til Julius Caesar.¹⁸

Den andre metoden var substituering. Enklest kan dette gjøres ved å erstatte alfabetet med et nytt alfabet hvor bokstavene oppstilles i en tilsynelatende helt vilkårlig rekkefølge. Det er en litt vanskeligere kode å knekke, men en tilsvarende metode finner vi allerede i Hellas på 300-tallet før vår tidsregning, hvor alle vokalene ble erstattet med prikker, slik at A ble erstattet med en prikk i teksten, E med to prikker osv.¹⁹ Uansett hvilke system man benytter seg av betyr det at en bokstav erstattes med en annen i følge en fast regel eller nøkkel.

Denne metode ble mer raffinert når man vekslet mellom flere alfabetiske substitusjoner. De få manualer og lærebøker i kryptologi som eksisterte opp til annen verdenskrig viet mest oppmerksomhet mot slike fler-alfabetiske koder (og vi snakker altså om millioner mulige kombinasjoner). Under annen verdenskrig ble denne substitueringen eller chifreringen foretatt av maskiner. Både Enigma-maskinene hos tyskerne og Purple-maskinene hos japanerne ble knekket av de allierte, og det var avgjørende både for slaget om Atlanterhavet, som vi skal se, og for amerikanernes krigføring i Stillehavet. Hvis vi skal sammenligne datidens kryptoanalytikere med en gruppe personer som kan få en tilsvarende viktig oppgave i en fremtidig krig, vil det være hackere. Disse vil imidlertid ikke bare nøye seg med å bryte inn i informasjonssystemene for å stjele informasjon - de vil også lett kunne manipulere denne. Under Kosovo-konflikten i 1999 brøt f eks en gruppe som kalte seg den 'serbiske internett hæren' seg inn på albanske hjemmesider på internett og endret innholdet for å bakvaske albanerne²⁰. Slektskapet er faktisk enda tettere enn mange tror. Alan Turing, sjefskryptograf i Bletchley Park fra 1943 og mannen som knekket den tyske krigsmarinens Enigma-signaler, var den første som, i 1936, formulerte det konseptuelle eller teoretiske grunnlaget for den universelle regnemaskinen eller 'datamaskinen' i vårt språk. Den modellen var avgjørende for å gi en annen ny vitenskapelig disiplin som oppsto like etter krigen - *kybernetikken* - et konkret innhold. De to første stavelen i dette ordet finner vi igjen i *cyberspace* og *cyberwar*. Dette vil jeg komme tilbake til senere.

6 Informasjonsdominans og slaget om Atlanterhavet

Slaget om Atlanterhavet kan betraktes som "et slag mellom fartøyer, fly, radar, radiotelegrafi, taktikk, sjømannskap – og kryptoanalyse. Tyskerne leste kodene til de britiske konvoiene med

ødeleggende konsekvenser; britene leste kodene til de tyske ubåtene gjennom Ultra-prosjektet med like ødeleggende konsekvenser.”²¹

Året 1943 åpnet med flere tyske ubåter enn noen gang tidligere. Gang på gang måtte britene gripe inn for å hindre at amerikanerne angrep ubåter på basis av Ultra-etterretninger alene, noe som ifølge britene ville fått Dönitz til å konkludere at Enigma-maskinen ikke lenger var usårbar. Det interessante med denne problemstilling, er at de allierte ikke kunne utnytte sin informasjonsoverlegenhet eller -dominans fordi tyskerne med enkle mottiltak kunne eliminere den. Den paradoksale utfordring for Admiralitetet og *Submarine Tracking Room* var å gi direktiver og etterretninger til de taktiske sjefene på havet på en slik måte at taktikken ikke skulle røpe at britene visste hvor ubåtene befant seg!

Det viste seg å være en umulig oppgave å sikre konvoiene under disse forutsetningene. I mars 1943 lider de allierte noen enorme tap i to konvoier. Ubåtene måtte ødelegges før de kom på skuddhold av konvoiene. I april da Ultra avslørte at 98 ubåter seilte ut i Atlanterhavet – det meste Dönitz noen gang hadde sendt ut på en gang – var det derfor avgjørende å foreta endringer i strategien. Andre teknologiske nyvinninger gjorde dette mulig, samtidig som Ultra-hemmeligheten kunne bevares. Den viktigste av disse var H2S, den første 10-cm radar. Den hadde en usett rekkevidde og nøyaktighet og som en cm-radar var det umulig for ubåtenes radarvarslingsystem, *Metox*, å oppdage den.

Alle taktiske sjefer, britiske og amerikanske, ble anbefalt å senke enhver ubåt uansett hvor den var lokalisert. Frigjort fra lenkene som var knyttet til Ultra, ble flyene fortalt hvor ubåtene var over radiotelegrafi fra *Submarine Tracking Room*. Ved så å bruke den nye radaren var de i stand til å bestemme nøyaktig ubåtenes posisjon, selv om natten, og angripe.

Selv så sent som i 1959 da Dönitz utga sine erindringer, nektet han å tro at hans koder var blitt kompromittert. Han tillot den katastrofe som rammet hans utbåter den britiske radars fortrefelighet.²² Liddell Hart bekrefter i sitt store verk om annen verdenskrig denne oppfattelse når han sier at ”den nye 10-cm radar – som ubåtene ikke kunne oppfange - var den viktigste blant bedriftene til de britiske vitenskapsmennene.”²³ Ultra var hemmeligstemplet helt frem til 1974. Betydningen av denne form for krigføring har derfor ikke fått den plass den fortjener i de fleste krigshistoriske og militærteoretiske fremstillingene.

Slaget om Atlanterhavet viser flere interessante forhold som er knyttet til begrepet informasjonsdominans. For det første viser det at det å ha det beste situasjonsbildet ikke er tilstrekkelig for å slå en motstander - de taktiske virkemidlene må brukes på en slik måte at denne dominans kan utnyttes. Det viser videre at kildene bak en slik informasjonsdominans kan være så følsomme at høyere nivå tvinges til å holde informasjon som er vital for de taktiske sjefene, tilbake. Det antyder også at en informasjonsdominans som alene er basert på elektronisk etterretning vil være sårbar for mottiltak.

Det å tilstrebe en best mulig informasjonsoversikt eller -dominans og samtidig hindre en motstander tilstrekkelig informasjon, er en viktig forutsetning for at en militære operasjonen skal lykkes. Men som tidligere nevnt, er det ikke et mål i seg selv - det er et middel for å forstå hva som skjer, og ut fra denne kunnskap foreta de riktige handlinger før en motstander får tid til å reagere. Forestillingen om en total informasjonsdominans over en motstander er en illusjon - det er en logisk umulighet som vi hele tiden må være oss bevisst for å unngå ubehagelige overraskelser.

Informasjonsdominans skal gi oss kunnskap om 'stridsrommet' som om det er avgrenset i rom og tid. Den kunnskap består av fire typer²⁴. Først den kunnskap som er etablert ut fra hva vi vet at vi vet. Det er uttalt kunnskap. For det andre den kunnskap som er etablert ut fra det vi vet at vi ikke vet. Det er uttalt uvitenhet. Sammen utgjør disse tilsynelatende et perfekte utgangspunkt for å bestemme hva informasjonsoperasjonen skal fokusere mot - nemlig å skaffe oss den kunnskap vi vet vi mangler. Dette er uttrykk for en rent symmetrisk oppfattelse av krig - det at enhver motstander tenker og handler som oss. General Westmoreland, sjefen for de amerikanske styrkene i Vietnam, ble beskyldt for et slikt "selvbedrag" ved at han "utviklet en strategi som passet hærens foretrukne [operasjonsmåte], styrkestruktur og doktrine”²⁵.

Det finnes imidlertid to andre former for kunnskap. Den sorte typen. Den første har å gjøre med hva du ikke vet at du faktisk vet. Ikke før du står overfor en ny situasjon og handler, vil du finne ut om du faktisk er i stand til å håndtere den. Det er taus kunnskap og kanskje det som kommer nærmest begrepet *intuisjon*. Til slutt finnes det noe som kjennetegnes ved at du ikke vet at du ikke vet. Det er taus uvitenhet. Det er et spesielt interessant område. Vi taler om et område hvor det ikke finnes noe kjent handlingsmønster - derfor vet vi verken hva slags informasjon vi skal lete etter eller hvilken kunnskap om oss vi må sikre eller skjule. Vi vet følgelig heller ikke hvilke virkemidler vi skal bruke til det ene eller til det andre. Det er et typisk uttrykk for en asymmetrisk situasjon - hvor en motstander handler på en måte som for oss er fullstendig uventet og bruke virkemidler og metoder vi ikke i vår villeste fantasi kunne forestille oss, eller egentlig bare der! Informasjonsdominans vil altså i beste fall alltid være relativ, i verste fall fullstendig irrelevant.

7 Krigføring i det kybernetiske rom

Intet av det jeg hittil har sagt tyder på at informasjonsoperasjoner og problemer knyttet til denne type operasjoner er av særlig ny dato. Det finnes imidlertid en utviklingstrend i samfunnet generelt som sannsynligvis vil gjøre informasjonsoperasjoner til et langt viktigere strategisk virkemiddel enn det vi har sett hittil - nemlig utviklingen av globale og regionale datanettverk som reduserer - men ikke fjerner - betydningen av territorier, avstander og tid.

Når Fuller betegnet de elektroniske oppfinnelsene i 1940-årene for den tredje industrielle revolusjon, kan vi betegne de mikro-elektroniske oppfinnelsene på 1970-tallet for den femte, eller snarere en post-industriell revolusjon. Forutsetningene for denne revolusjon går, som tidligere nevnt, tilbake til 1930- og 40-årene hvor det konseptuelle grunnlaget legges ved utviklingen av Turings modell for en universell computer og Norbert Wieneres etablering av *kybernetikk* som en ny vitenskapelig disiplin. Begge deler kan virke utrolig abstrakte for vanlige mennesker, men hvis vi sier at begge beskriver en ikke-fysisk virkelighet hvor kommunikasjon i digitale koder brukes for å kontrollere og regulere maskiner, befinner vi oss i en verden hvor *informasjon* og *logikk* er viktigere enn *kinetisk energi* og *fysisk materiale* for å forklare hvordan systemene der blir påvirket. Det typiske eksempel på denne ikke-fysiske eller *virtuelle* virkelighet er den elektroniske informasjon som produseres og formidles i datamaskiner, telekommunikasjonssystemer og datanettverk, som f.eks. internett. Data-, radar-, TV-skjermen osv. representerer grensesnittet mellom den virtuelle og fysiske verden. Og det interessante for oss er at alle disse skjermene kan manipuleres uten at vi kan se det. Denne virtuelle virkelighet eksisterer i det kybernetiske rommet eller *cyberspace*, og det har alltid eksistert, men ikke før mennesket oppfant teknologier som opererte i det elektromagnetiske spektrum ble det "synlig" og lagt merke til. I dag blir stadig flere samfunn, selskaper og militære organisasjoner totalt avhengig av det som foregår i dette grenseløse rommet for å løse sine oppgaver. Virksomheten i dette rommet utgjør et klart definert mål for en aggressor, blant annet fordi en angriper ikke behøver fysiske maktmidler, men primært logiske og matematiske evner. Det representerer derfor en betydelig sårbarhet.

Det kybernetiske rommet kan f.eks. påvirkes gjennom 'våpen' som 'algoritme'-bomber, som forvrenger et stykke av en algoritme (altså en regneoperasjon) slik at programvarens evne til å utføre den funksjon den var tiltenkt begrenses. Det kan kanskje sammenlignes med å forvrengte grammatikken i en setning slik at noe av teksten fremstår som uforståelig - vi vil imidlertid som regel oppdage at noe er galt - det vil ikke en computer. Et annet 'våpen' kan være 'programvare'-bomber som føyer til en uønsket algoritme som begrenser iverksettelsen av programvare-funksjoner eller styrer dem til å foreta beregninger som ikke var tillatt av den programvare som opprinnelig var lastet inn. Det kan sammenlignes med å føye til nye avsnitt i en ordre uten at mottakeren er klar over det. Datavirus i allslags varianter kan være andre 'våpen'.

8 Informasjonsoperasjoner og folkeretten

Et av de gjennomgående trekk når det gjelder utviklingen av krigens folkerett, er at straks krig eller samfunnet generelt har beveget seg inn på et nytt område, har lovverket ligget på etterskudd.

Hvis vi forsøker undersøker hvilket forhold folkeretten og spesielt krigens folkerett har til informasjonsoperasjoner og informasjonskrigføring, støter vi på en rekke problemstillinger hvor det er behov for avklaring. Det gjelder kanskje først og fremst bruk eller misbruk av det kybernetiske rommet for å ramme eller ødelegge en motstander. Vi har rimelig klare definisjoner av hvem som er 'kombattanter', hva 'maktbruk', 'væpnet angrep' og 'væpnet aggresjon' betyr i den fysiske verden. Men hvordan definere disse begreper i den virtuelle verden - når angrepet kommer gjennom eteren og mot infostrukturen?

Når det gjelder virkningene av denne type operasjoner eller krigføring, er krigens folkerett eller den humanitære folkeretten like bindende som ved bruk av fysiske maktmidler. Det å bestemme hvem som er kombattanter eller stridende har alltid vært problematisk, hvis vi ser bort fra rent symmetriske og begrensede kriger. Er en *hacker* en kombattant? Opererer han alene i fredstid og rammer, ødelegger eller stjeler fra en kilde, er han en forbryter. Gjør han det samme som ledd i en stats informasjonsoperasjon mot en fysisk aggressor, er han i samme posisjon som mange av de 6000 'sivilt' ansatte som arbeidet for å knekke de tyske hemmelige kodene i Ultraprojektet under annen verdenskrig. Problemet her som i alle andre sammenhenger er gråsonen mellom den klare forbryter og den som under krig er ansatt for direkte å bidra til at de militære operasjonene lykkes.

Når det gjelder andre begreper som f eks 'væpnet angrep' og 'maktbruk' gir allerede FN-pakten muligheter for å bruke eteren for å straffe en aggressor. Artikkel 41 lister en rekke tiltak som Sikkerhetsrådet kan treffe mot en som truer den internasjonale fred og sikkerhet, blant annet avbrytelse "post, telegraf, radio og andre kommunikasjonsmidler." Det interessante er at pakten åpenbart oppfatter denne form for straffetiltak som mildere enn bruk av militære styrker (art. 42). Det må dog sies at opphavsmennene neppe visste hvilke konsekvenser det i dag kan få hvis infostrukturen avbrytes eller forstyrres (uttrykket som brukes, *interrupt*, betyr begge deler). Men hva som er tillatt å gjøre f eks mot sivilbefolkningen, uansett hvilke midler vi bruker, er rimelig godt behandlet i den humanitære folkeretten.

Hovedproblemet for folkerettsjuristene er kanskje først og fremst de tilfellene hvor en stat eller en ikke-statlig aktør (f eks Microsoft) bruker informasjonsoperasjoner for å fremme eller sikre sine interesser, uten å synliggjøre operasjonen ved samtidig å bruke fysiske, økonomiske eller diplomatiske maktmidler. Russerne hevdet f eks allerede i 1991 at det franske luftforsvarssystemet som var solgt til Irak hadde innlagte 'logiske bomber' som gjorde det ubrukelig mot de multinasjonale styrkene under kampooperasjonene i Golfen²⁶. Denne type operasjoner, hvis de forekommer - noe vi nok dessverre må anta - vil være så hemmelige at ingen vil kunne bevise at de foregår. Det vil igjen være som ved Ultraprojektet som forble en britisk hemmelighet frem til 1974 - 29 år etter krigens avslutning.

Når det gjelder bruk av denne type virkemidler, er det nok et forhold som er enda viktigere enn folkeretten - nemlig det etiske.

Hvis en stat eller en ikke-statlig aktør misbruker sin informasjonsteknologiske makt ved å plante 'logiske bomber' i kommersielle og militære systemer som selges på verdensmarkedet, og bruker 'hacker'-metoder rimelig ukritisk og i hemmelighet for å fremme sine interesser, vil det kunne få uforutsigbare konsekvenser for verdenssamfunnet og for forholdet mellom dets aktører. Tillit som en av de mest fundamentale hjørnesteinene i vår sivilisasjon vil gå tapt. En snikende utvidelse av informasjonsoperasjoner til også å omfatte det sivile samfunn vil tilsløre eller utviske grensene mellom den daglige konkurransen og ikke-erklært krigføring.²⁷ Denne form for 'krigføring' vil dessuten kunne legitimere terrorisme - når stater eller store selskaper har lov - hvorfor har ikke personer eller grupper som står utenfor den etablerte orden lov?

9 Informasjonsoperasjoner i fredsstøttende operasjoner

Fredsstøttende operasjoner dekker et vidt spekter av aktiviteter hvor det militære virkemidlet har forskjellige funksjoner. Fra politi-lignende oppgaver i tradisjonelle fredsbevarende operasjoner via forskjellige støtteoppgaver knyttet til diplomatisk virksomhet i fredsskapende og fredsbyggende operasjoner til rene kampfoppdrag i fredsopprettende operasjoner. Et viktig kjennetegn ved denne type operasjoner er at militære styrker i utstrakt grad må forholde seg til andre ikke-militære aktører innenfor operasjonsområdet - både vennligsinnede, i utgangspunktet nøytrale og fiendtlig innstilte.

Fordi omgivelsene for fredsstøttende operasjoner er så komplekse, som antydnet, og fordi de gjennomføres med mediernes søkelys konstant rettet mot virksomheten, er det viktig at den strategiske bakgrunnen for det internasjonale samfunns inngripen, om det så er FN, NATO eller andre organisasjoner, og formålet med bruk eller manglende bruk av forskjellige virkemidler, formidles og forstås av alle involverte parter. Det forutsetter en felles informasjonsstrategi og en felles forstått og etterlevd policy for informasjonsoperasjoner.

NATO har under sine operasjoner hittil ikke hatt en slik policy, men har i de siste år arbeidet med et slikt dokument. En av de største utfordringene fra militær side er forholdet til den sivile siden, det være seg lokalbefolkningen, massemediene, andre statlige og ikke-statlige organisasjoner i området, og forhold til hjemmeopinionen.

En forutsetning for en vellykket strategi for en informasjonsoperasjon i denne type operasjoner, vil være å koordinere tre sentrale aktiviteter. For det første PR-virksomheten, den virksomhet som er rettet mot lokale og internasjonale medier for å forklare og rettferdiggjøre på en troverdig måte hvorfor operasjonen gjennomføres. For det andre de psykologiske operasjoner, som har til formål å påvirke lokalbefolkningen og de lokale lederne til en vennligsinnede holdning overfor de internasjonale styrkenes tilstedeværelse og virksomhet. Og for det tredje sivil-militært samarbeid som har til formål å samordne informasjonen til lokalbefolkningen om formålet med den sivile og militære innsatsen i operasjonsområdet samt å sende positive signaler til den samme befolkning og ikke-statlige organisasjoner i området gjennom støtte til viktige funksjoner - for eksempel gjennom tilbud om transport-, sambands-, sanitets-, og ingeniørstjenester. Denne siste aktiviteten har ofte blitt oppfattet med en betydelig mistenksomhet fra militær side ut fra frykt om utglidning av det militære oppdraget.

Informasjonsoperasjoner er ikke et fenomen som bare det internasjonale samfunn benytter seg av. Aktørene i de konflikter vi griper inn for å håndtere, har som regel et meget godt organisert apparat nettopp for denne type aktiviteter. De bosniske serberne under Karadzic var nærmest hundre prosent koordinert i sine militære, politiske og medieutspill.²⁸

Journalistene og redaktørene i det kroatisk TV hadde for 1993 en håndbok som fortalte hvordan de skulle omtale henholdsvis serbere og muslimer i Bosnia. Denne endret seg ettersom alliansene mellom serbere, muslimer og kroater skiftet under krigen. I en periode skulle serberne omtales som "byzantinske barnespisende vampyrer" og muslimene som "blomsten av det kroatisk folk". Etter at alliansene hadde skiftet skulle bosnia-serberne omtales som "den allierte serbiske hær" og muslimene som "den europeiske jihads slagterenheter"²⁹.

En annen form for informasjonsoperasjon, som ikke er helt åpenbar ved første øyekast, noe som gjør den ekstra virkningsfull som et informasjonsvåpen, forteller David Owen om. Om Sarajevo i 1993 sier han at det ble stadig klarer at det var to beleiringer av byen: en av den bosnisk-serbiske hæren med granater, snikskyttere og blokader, og den andre av den bosniske regjeringshæren med indre blokade og byråkrati som hindret deres eget folk i å forlate byen. I en radioutsending sa hæren - ikke regjeringen - at stridsdyktige menn i alderen 18-65 og kvinner i alderen 18-60 hadde forbud mot å forlate [Sarajevo] fordi de skulle brukes i forsvar av byen. Men den egentlige grunnen var en annen. I propagandakrigen høstet den serbiske beleiringen verdens sympati, og for [å opprettholde denne sympati] hadde de behov for at de gamle og barn ble i byen. Den var deres mest følelsesladede propaganda våpen for å få amerikanerne til å kjempe i krigen, og de ønsket aldri å svekke det³⁰.

10 Avslutning

Jeg har nå forsøkt å gi en smakebit på hva som ligger i begrepet informasjonsoperasjoner. Det har jeg gjort ved bruk av en rekke eksempler fordi jeg mener det er en bedre metode enn å ramse opp en rekke definisjoner. Jeg har forsøkt å fremheve noen sider ved informasjonsoperasjoner som, jeg mener, det er viktig å ta hensyn til når vi betrakter Forsvaret som et sikkerhetspolitisk virkemiddel.

For det første har alt hemmelighold omkring viktige aspekter knyttet til informasjonsoperasjoner ført til at disse kapasiteter er blitt sterkt nedtonet og sannsynligvis undervurdert i debattene om forsvarsstrukturen.

For det andre viser eksemplene at bruk av denne type operasjoner og virkemidler ofte er en forutsetning for at de konvensjonelle militære styrkene skal kunne gjennomføre en vellykket kampanje eller operasjon.

For det tredje viser eksemplene at informasjonsoperasjoner består av sivile og militære operasjoner og kapasiteter som både kommer i tillegg til og som støtter det militære virkemidlet over hele spekteret fra fred til krig. Det fordrer en tett koordinering mellom sivile og militære virkemidlene

For det fjerde viser flere av eksemplene at informasjonsoperasjoner er et meget kosteffektivt virkemiddel hvis det brukes riktig, både når det gjelder å redusere tap av mennesker og materiell.

Til sist viser den skisserte utviklingen at slik de moderne samfunn, herunder militærmakten utvikler seg, i retning av nettverkssentrerte strukturer, blir disse mer sårbare for kybernetisk krigføring. Men denne utvikling medfører også at vi sannsynligvis vil få en vektforskyvning i de militære strukturer fra kinetiske våpen, fysisk styrker og mye materiell til større vekt på kapasiteter til å gjennomføre effektive informasjonsoperasjoner.

¹ Sun Zi (Sun Tsu), *Kunsten å krige*, oversatt av Harald Bøckman, Gyldendal Norske Forlag ASA 1999; s. 40

² Op.cit.; s. 33

³ Forsvarets fellesoperative doktrine (FFOD) definerer kommando- og kontrollkrigføring (C2W) på følgende måte: "Den integrerte bruk av alle militære kapasiteter, herunder operasjonssikkerhet (OPSEC), villedning, psykologiske operasjoner (PSYOPS), elektronisk krigføring (EK) og fysisk ødeleggelse for å påvirke, svekke, ødelegge eller nekte informasjon til en motstanders kommando- og kontrollsystem, og for å beskytte vårt eget mot tilsvarende virksomhet."

⁴ Kuehl, Dan, "Strategic Information Warfare: A Concept", *Militært tidsskrift*, nr 1-1999; s. 56

⁵ "Memorandum for the president", 18 June 1944 (<http://www.academic.marist.edu/psf/psfa55/a55m03.htm>)

⁶ Lipset, David, Gregory Bateson: The Legacy of a Scientist, Boston: Beacon Press 1982; s.174

⁷ Kuehl, Dan, Op.cit.; s. 59

⁸ Owen, David, *Balkan Odyssey*, London; Indigo 1996; s. 125-26

⁹ Op.cit; s. 89-90

¹⁰ van Creveld, Martin, *Command in War*, Harvard University Press 1985; s. 154

¹¹ Brown, Anthony Cave, *Bodyguard of Lies*, London: A Howard & Wyndham Company 1976; s. 525

¹² Fuller, J. F. C., *The Conduct of War 1789-1961*, London: Methuen & Co Ltd 1961 og 1979; s. 313

¹³ Op.cit.; s. 99

¹⁴ Clausewitz, Carl von, *Vom Kriege*, Frankfurt: Ullstein GmbH 1980; s. 18-19

¹⁵ Paddock Jr., Alfred H., "Robert Alexis McClure: Forgotten Father of Army Special Warfare", *Special Warfare*, Fall 1999; s. 3

¹⁶ Op. cit.; s. 8

¹⁷ Hodges, Andrew, *Alan Turing: the Enigma*, London 1983; s. 198

¹⁸ Hodges, Andrew, Op.cit.; s. 162

¹⁹ Xenofon/Aineias, *Fra antikkens krigskunst*, oversatt av Inge Tjøstheim, Oslo: Aschehoug & Co, 1994; s 140

-
- ²⁰ Bieber, Florian, "Cyberwar or Sideshow? The Internet and the Balkan Wars", *Current History*, March 2000; s. 127
- ²¹ Brown, Anthony Cave, Op. cit.; 251
- ²² , Op cit.; s 259
- ²³ Liddell Hart, B. H., *History of the Second World War*, New York: Da Capo Press 1999 (1971); s. 385
- ²⁴ Wik, Manuel W, "Mobilization for a new era", *Militært tidsskrift*, nr 1-1999; s. 32
- ²⁵ McNamara, Robert S., *In Rerospect: The Tragedy and Lessons of Vietnam*, New York: Vintage Books 1996; s. 211
- ²⁶ Thomas, Timothy L. , "Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations", *The Journal of Slavonic Military Studies*, Vol. 1, No. 1 (March 1998); s 58
- ²⁷ Wik, Manuel W, Op. Cit.; s. 35
- ²⁸ Wentz, Larry K., Peace Operations and the Implications for Coalition Information Operation: The IFOR Experience, (Working Draft 2/18/98), http://www.dodccrp.org/bo_infooop1.htm; s. 8
- ²⁹ Sørensen, Durdica Z. Og Bjørn, Anders, *Den jugoslaviske krig*, Forlaget Amanda 1996; s. 167
- ³⁰ Owen, David, Op. Cit.; s. 63