Internasjonal POLITIKK Årgang 71 | Nr. 2 | 2013 | 241–251 | ISSN 0020-577X

FOKUS: CYBERSPACE

Cyberkrigføring og Forsvarets operative evne

ROGER JOHNSEN
Sivilingeniør, oberstløytnant og sjef, Forsvarets ingeniørhøgskole
rojohnsen@gmail.com

Informasjons- og kommunikasjonsteknologien har i løpet av de siste 20 år endret samfunnet. På den ene siden bidrar IKT til økonomisk vekst, økt velferd og effektivisering av offentlig sektor. På den andre siden oppstår nye utfordringer i form av cyberkriminalitet, trusler mot personvernet og ivaretakelse av individuelle rettigheter (Sabbagh et al. 2012). Tilsvarende bidrar IKT til utvikling og skaper utfordringer også i forsvarssektoren. Hvordan bør så småstaten Norge innrette Forsvaret for å utnytte cyberteknologien og samtidig håndtere det nye trusselbildet? Dette bidraget diskuterer hvordan økt cyberkapasitet vil kunne påvirke Forsvarets operative evne, med fokus på anvendelse av militær makt i og gjennom cyberdomenet. Det konkluderes med at Forsvaret må gjennomgå betydelige endringer for å kunne utnytte den nye teknologiens potensial.

Alberts et al. (2001) har i sine studier av Network Centric Warfare (nettverksbasert forsvar) påvist en klar sammenheng mellom informasjonsdeling, situasjonsbevissthet, samarbeidsevne og militær effekt. Gjennom å utvikle Forsvaret i en nettverksbasert retning, vil dermed tempo og presisjon forbundet med lokalisering og engasjement av mål kunne forbedres radikalt. IKT øker således ikke bare kampkraften, men bringer en helt ny dimensjon inn i krigføringen. Som et eksempel vil en fregatt kunne lede bekjemping av mål, lokalisert av en rekognoseringsstyrke på land, ved hjelp av missiler fra et kampfly. Utviklingen omtales som nettverksbasert forsvar, hvor nye og effektive organisasjons- og ledelsesformer blir mulige gjennom smart bruk av IKT.

Siden en forventer at IKT kan utgjøre en formidabel styrkemultiplikator, er det logisk å anta at informasjonsinfrastrukturen vil bli betraktet som et operativt tyngdepunkt av fremtidige motstandere. Motivasjonen ligger i at angrep i cyberdomenet har potensial for å gi store fordeler i de

fysiske domenene (Skar 2006). Samtidig forsterker cyberdomenet avhengighetene mellom sosial, politisk, økonomisk og militær virksomhet. Aktør- og trusselbildet i nåtidens konflikter blir dermed svært sammensatt og dynamisk, noe «den arabiske våren» er et konkret eksempel på (Al-Jazeera 2012). Tilsvarende ser man at autoritære regimer utøver makt gjennom å kontrollere media, internett og telekommunikasjon (CNN 2011).

Cyberdomenet utgjør således et nytt område for militær makt og stiller nasjonalstaten overfor en ny trusseldimensjon. Analysen i denne artikkelen utfordrer den etablerte sikkerhetstenkningen og beskriver en militærtaktisk tilnærming til utfordringene. I artikkelens første del diskuteres konsekvensene av cybertrusselen. I andre del utdypes grunnlaget for militære operasjoner i cyberdomenet. Til slutt beskrives en mulig løsning for å utnytte teknologien effektivt og forsvare systemene mot cyberangrep.

Sikkerhet i en ny kontekst

Dette bidraget tar utgangspunkt i at cyberkrig er en reell mulighet, og at en militær cyberkonflikt vil være å forstå som «krig». Clausewitz' (1832) tese om at krig er en forlengelse av politikken med andre virkemidler, har fått fornyet gyldighet i diskusjonen rundt cyberkrigføring. Clausewitz understreket også krigens voldsaspekt og fysiske ødeleggelse. I sin definisjon av cyberkrig har Lewis (2011) i så måte lagt seg på en clausewitzisk linje. Han definerer cyberkrig som «*bruk av cyberteknikker i den hensikt å forårsake skade, materiell ødeleggelse eller tap av menneskeliv for å oppnå politiske mål utført av stater eller politiske grupper*». Med utgangspunkt i Lewis kan vi utlede at cyberteknikker vil kunne falle innunder definisjonen av krig eller væpnet makt.

Tradisjonelt har Forsvaret forholdt seg til trusselen mot sine IKT-systemer ved hjelp av forebyggende sikkerhetstiltak. En tilnærming som i utgangspunktet virker fornuftig, da intensjonen er å forhindre at skade oppstår. Under dette paradigmet forutsettes det at eieren av systemene identifiserer og fjerner alle tekniske svakheter, og etablerer sikkerhetstiltak som stanser forsøk på ødeleggelse eller spionasje. For et nettverksbasert forsvar, hvor avanserte informasjonssystemer og høyteknologiske våpensystemer er tett integrert i virksomhetsprosessene, vil det imidlertid ikke la seg gjøre å identifisere alle sårbarheter (Jones & Ashenden 2005). Angrep vil komme der vi er minst forberedt og virkningen samtidig er tilstrekkelig (Helpern & Tuttle 1993).

Avgrenser den defensive part seg til tradisjonell forebyggende sikkerhet, vil han altså stå overfor en umulig problemstilling. Selv om han er i stand til å utbedre kjente svakheter, vil han ikke evne å avdekke alle sårbar-

heter. Aggressoren vil derfor ha et betydelig fortrinn ved å kunne kartlegge motpartens informasjonsinfrastruktur og tilhørende forebyggende sikkerhetstiltak, for deretter selv velge tid og sted for å angripe. Reagerer forsvareren på risikoen ved selv å begrense utbredelsen eller egen bruk av IKT, vil egen militær evne reduseres samtidig.

Situasjonen kan på mange måter sammenlignes med de tyske mekaniserte manøverstyrkene som enkelt omgikk den sterkt befestede Maginotlinjen i innledningen til 2. verdenskrig. Selv om flere væpnede konflikter i mellomkrigstiden hadde blitt gjennomført som «bevegelseskriger» med lette og mobile styrker, tilla ikke Frankrike disse felttogene noen vesentlig betydning. Kombinasjonen av krigstretthet og konservatisme ledet derimot til at franske sivile og militære myndigheter valgte å holde seg til erfaringene fra den regulære krig på vestfronten. Mens den tyske rustningsmaskinen bygde stridsvogner og fly og trente sine styrker i manøverkrig, valgte Frankrike å stille enorme bevilgninger til rådighet for med all tilgjengelig teknologi å gjøre den fransk-tyske grensen ugjennomtrengelig (Ruge 1946).

Det er derfor avgjørende at man både anerkjenner hvor sentral informasjons- og kommunikasjonsteknologi er for militær virksomhet i det 21. århundre, og at forebyggende sikkerhetstiltak er utilstrekkelige i væpnede konflikter. Anskaffelse og bruk av IKT i Forsvaret er derimot fortsatt regulert av et lovverk som utelukkende er innrettet mot forebyggende sikkerhet.

Cyberoperasjoner

På strategisk nivå er gjerne den politiske målsettingen defensiv av natur. En stat uten imperialistiske ambisjoner vil gjerne ha som mål for sin sikkerhetspolitikk å opprettholde territoriell integritet, sikre nasjonale interesser og kunne motsette seg tvangsdiplomati. Militærmakten er derimot avhengig av å kunne gjennomføre så vel offensive som defensive operasjoner for å oppnå den defensive politiske målsettingen.

Defensive militære operasjoner kan, som et absolutt maksimum, kun bidra til å opprettholde utgangspunktet. Lykkes aggressoren i sin offensiv, vil forsvareren måtte angripe for å gjenopprette det tapte. Tradisjonelt er derfor angrepsstrid ansett som eneste mulighet for å oppnå et fordelaktig utfall. Krigføringen vil således karakteriseres av vekselvirkningen mellom angreps- og forsvarsoperasjoner. Forsvarsstrid i ett domene kan muliggjøre offensive operasjoner i et annet domene, eksempelvis hvor defensive cyberoperasjoner gjennomføres for å skape forutsetninger for angrep i luft-, land- eller sjødomenet.

Effekten av defensive og offensive tiltak vil variere over tid. Fuller (1932) beskriver dette fenomenet som den konstante taktiske faktor, hvor

forbedring av våpenteknologi resulterer i at motstanderen utvikler mer avansert beskyttelse som gjør den opprinnelige forbedringen foreldet. Han gir oss her et bilde av en evolusjonens pendel som, sakte eller raskt, vil svinge fra det offensive til det beskyttende og tilbake igjen i takt med den sivile utviklingen; hvor hver svingning i målbar grad eliminerer fare. Favorisering av cyberoffensiven i en tidsperiode må derfor antas å imøtegås av effektive defensive cyberteknikker i en senere periode.

Som vi tidligere har vært inne på, utelukker ikke en defensiv ambisjon bruk av offensive virkemidler. For å svekke aggressorens kapasiteter i land-, sjø- og luftdomenet, kan det derfor være hensiktsmessig å ramme ham i cyberdomenet. Tilsvarende er det fundamentalt å kunne avsløre fiendtlige cyberangrep i en tidlig fase. Gjennom etterretning mot fienden og overvåking av egne IKT-systemer vil skjermingstiltak kunne iverksettes, eventuelt kombinert med operasjoner for å ramme eller forstyrre fiendens cyberkapabiliteter.

Cyberdomenet tilbyr her en unik mulighet til å forme lendet til forsvarerens fordel. Cyberlendets topologi kan endres samtidig som kapasiteter, funksjonalitet og tilgang til informasjon opprettholdes. Taktisk tilpasning av cyberlendet kan gi flere effekter. For det første kan dynamiske sperre- og overvåkingstiltak gjøre vitale deler av infrastrukturen og funksjonaliteten enklere å forsvare. For det andre vil endringer i infrastrukturen kunne svekke både presisjonen og virkningen av fiendens offensive cyberteknikker.

Defensive tiltak vil derimot ikke alene kunne gjenopprette en situasjon hvor fienden har fremgang eller er i ferd med å ødelegge forsvarerens kapasiteter. Velger eller tvinges forsvareren til å la aggressoren opprettholde initiativet, vil han komme i stadig større ubalanse. Aggressoren kan dermed gradvis og uforstyrret omgå eller trenge gjennom permanente og statiske forsvarstiltak. På denne måten vil forsvareren kunne tvinges til å oppgi egen bruk av cyberdomenet og fratas kontrollen med egne ledelses- og våpensystemer. Ambisjonen med defensive cyberoperasjoner bør derfor ikke avgrenses til å forhindre at fienden trenger inn i våre systemer, men snarere innrettes mot å forhindre at han lykkes i å frata oss vår operative handlefrihet. Offensiv opptreden fremstår derfor som et sentralt prinsipp også i defensive cyberoperasjoner. Gjennom å forstyrre fiendens ledelsesapparat, etterretningsenheter og støttefunksjoner, vil forsvareren kunne svekke aggressorens evne til å anvende sine cyberkapasiteter.

Vår egen avhengighet av IKT kombinert med en fiendes vilje og evne til å ramme oss i cyberdomenet, tilsier at vi bør forberede oss på å gjennomføre militære operasjoner med fienden til stede i vår informasjonsinfrastruktur. Cyberangrep kan ramme uten forhåndsvarsel, da det ikke er enkelt å observere styrkeoppbygging i cyberdomenet. Eskalering av konflikter krever heller ikke felles grenser eller fremføring av synlige militære styrker. Cyberdomenets egenart medfører derimot at angriperens fysiske

posisjon er lite relevant. Vi kan herunder utelede fire grunnleggende utfordringer ved defensive operasjoner i cyberdomenet: For det første å kunne stadfeste selve angrepet og ansvarliggjøre en aggressor. Dernest å kartlegge aggressorens cyberteknikker, metoder og mål. Videre å kartlegge skaden et angrep har forårsaket, og til sist utfordringen med å redusere aggressorens evne til å innvirke på vår bruk av cyberdomenet, samtidig som våre styrker fortsatt effektivt kan anvende egne systemer. I det følgende diskuteres en mulig tilnærming til disse utfordringene.

Cybertaktikk

Clausewitz (1832) definerer taktikk som anvendelse av tropper for å vinne slaget og strategi som utnyttelsen av slaget for å vinne krigen. Mer konkret kan taktikk forstås som prinsipper og metoder for å organisere og anvende militære styrker i strid. I forbindelse med planlegging av operasjoner legges styrkenes taktiske repertoar til grunn for mest mulig hensiktsmessig og effektivt å oppnå de militære målsettingene. Cybertaktikk blir dermed et spesialtilfelle av den generelle taktikken, tilpasset det politiske behovet for å utøve militær makt i eller gjennom cyberdomenet. Valg av taktisk doktrine vil således være førende for hvilke cyberstyrker Norge bør ha og hvordan disse bør utrustes og trenes.

Ansvaret for å forsvare Norge mot anslag og angrep gjør høyintensitets krigføring[1] til militærmaktens dimensjonerende oppgave. Samtidig muliggjør ikke forsvarsstrukturen militær tilstedeværelse i alle deler av norsk territorium. Kontinuerlig overvåking og evne til hurtig kraftsamling av militære ressurser og ild i hele ansvarsområdet, er derfor forutsetninger for å kunne forsvare Norge. Anskaffelsene av Nansen-klasse fregatter og F35 kampfly og digitaliseringen av Brigaden er ledd i å tilpasse innsatsfaktorene til denne virkeligheten. Kraftsamling forutsetter i sin tur samvirke mellom alle kapasitetene i en fellesoperativ ramme, altså samarbeid organisert på det nivå i Forsvaret hvor man ser forsvarsgrenene under ett. Formålet med Forsvarets IKT-investeringer er i så måte å sikre styrkene overlegen situasjonsforståelse og evne til effektiv koordinering og ledelse av tilgjengelige ressurser.

Overlegen situasjonsforståelse beskriver et relativt forhold mellom de stridende aktørene, hvor målet er å oppnå radikalt bedre oversikt over stridsfeltet enn motstanderen. Aktøren med den beste situasjonsforståelsen vil ha bedre forutsetninger for hurtigere å fatte mer hensiktsmessige beslutninger enn motstanderen. Situasjonsforståelsen muliggjør her at styrkene kontinuerlig kan lokalisere og identifisere mål. Nødvendig ild-

1. Kamphandlinger med konvensjonelle styrker i krig eller krigslignende situasjoner.

kraft kan deretter raskt allokeres fra den mest egnede våpenplattformen. Effekten vil være kumulativ, da den kan utnyttes for å påføre motstanderen stadig større skade, noe som igjen svekker hans situasjonsforståelse ytterligere. Cyberangrep vil i denne sammenheng kunne understøtte fysiske operasjoner gjennom å svekke motstanderens situasjonsforståelse, forstyrre hans våpensystemer eller begrense hans evne til å planlegge og lede militære operasjoner.

Innenfor dette paradigmet fremstår evne til å bygge ut systemer til støtte for egne styrker, utøve kontroll i cyberdomenet, overvåking av egne systemer og bruken av offensive cyberteknikker som grunnleggende elementer i en defensiv cybertaktikk.

Cyberstøtte

En nettverksbasert tilnærming til militære operasjoner forutsetter at datasystemene fungerer under så vel planlegging og forflytning av styrkene som under stridshandlinger. Evne til kontinuerlig informasjonsutveksling er en forutsetning for situasjonsforståelse, ledelse av operasjoner og styring av våpensystemer. De norske cyberstyrkenes mest grunnleggende oppgave blir derfor å etablere en fleksibel og robust informasjonsinfrastruktur til støtte for land-, luft- og sjøstridskreftene.

Operasjonsområdenes størrelse og styrkenes krav til mobilitet og informasjonsutveksling tilsier at behovet for informasjonsinfrastrukturer er omfattende. Cyberstyrkene må derfor være i stand til å utgruppere kommunikasjonssystemer i takt med operasjonene som gjennomføres. Ressursbehovet og risiko forbundet med etablering av egne taktiske kommunikasjonssystemer er betydelig. For å redusere belastningen på egne cyberstyrker og øke kapasiteten, vil det derfor være formålstjenlig å utnytte infrastruktur som allerede er tilgjengelig i operasjonsområdet. Spesielt er tilgang på satellittbaserte løsninger av interesse, da de gir mobile styrker fleksibilitet og tilbyr kommunikasjon inn i lite utbygde områder og over store havområder.

Informasjonsutveksling alene er derimot ikke et tilstrekkelig fundament for situasjonsforståelse og ledelse. Kompleksiteten i væpnede konflikter medfører at informasjon må analyseres og fortolkes for å kunne tillegges mening og skape forståelse. Mens datasystemene kan produsere store mengder ny informasjon, er det menneskene som tillegger informasjonen mening (Denning & Bell 2012). Militær ledelse blir dermed en kontinuerlig og interaktiv prosess uten deterministiske svar. Interaksjonen mellom IKT-systemene og soldatene utgjør her kanskje den viktigste funksjonen for å løse oppgaver verken datamaskiner eller mennesker kan utføre alene. En sentral oppgave for cyberstyrkene blir dermed å fort-

løpende tilpasse systemene, slik at de fleksibelt styrer informasjon til analytikere, beslutningstakere og avdelinger.

Cyberstøtte omfatter således de aktiviteter som direkte understøtter Forsvarets behov for situasjonsbevissthet, samarbeid, ledelse og styring av våpensystemer.

Cyberkontroll

En viktig utfordring for de norske cyberstyrkene er å sikre tilstrekkelig grad av kontroll med cyberdomenet. Cyberdomenets enorme kompleksitet gjør det umulig for forsvareren å avdekke alle sikkerhetshull i sine systemer. Kompleksiteten leder samtidig til at angriperen er avhengig av detaljerte etterretninger og rekognosering for å avdekke motstanderens kritiske sårbarheter. I denne sammenheng har Parks & Duggan (2011) vist at den part som har kontroll med informasjonsinfrastrukturen har en klar fordel. I væpnede konflikter vil det derfor være av vesentlig betydning å sikre seg kontroll over de deler av cyberdomenet som påvirker egne operasjoner.

I de fysiske stridsdomener angir en kontrollambisjon en tidsbegrenset evne til å nøytralisere eller fortrenge fienden fra et angitt geografisk område, slik at vi selv kan benytte området fritt. I cyberdomenet mister begrepet «område» mye av sin betydning da funksjonalitet, informasjon og kapasitet ikke nødvendigvis er låst til et geografisk område. Cyberdomenet kan derfor beskrives å være elastisk, da topografiske endringer av nettverkene ikke nødvendigvis fjerner disse verdiene.

Cyberdomenets elastisitet kan utnyttes til å forme «terrenget» til forsvarerens fordel. Gjennom en kombinasjon av sikkerhetstiltak, overvåking og dynamisk tilpassning av infrastrukturen vil fiendens muligheter for skjult infiltrasjon og angrep begrenses. Gis fienden derimot tid og mulighet til rekognosering, vil han på nytt kunne utvikle effektive angrepsteknikker. En sentral forutsetning for cyberkontroll vil dermed være egen evne til å forstyrre fiendens rekognoserings- og analysekapasiteter. Vi kan herunder utlede at ulike grader av cyberkontroll kan oppnås gjennom kombinasjoner av teknisk forsvarbarhet, systemovervåking og egne offensive cyberkapasiteter.

Cyberkontroll kan beskrives som en ambisjon om at egne styrker kan anvende cyberdomenet til angitte formål, uten vesentlig påvirkning fra fienden. Formål angir her hvilken funksjonalitet, kapasitet og informasjon kontrollambisjonen skal omfatte. Jo bredere formål, jo større usikkerhet om ambisjonen vil holde. Tilstrekkelig grad av cyberkontroll vil derimot være nødvendig både for å understøtte land-, sjø- og luftstridskreftene, og for å kunne projisere cybermakt mot en fiende. Graden av cyberkontroll vil derfor alltid være en balanse mellom ønsket operativ frihet og akseptabel risiko.

Cyberovervåking

Tilsvarende som for de fysiske arenaene for krigføring, er det nødvendig for Forsvaret å raskt identifisere etterretning og angrep i cyberdomenet. Virkningen av et cyberangrep kan derimot oppstå umiddelbart når det iverksettes. Tilpasning av egne forsvarstiltak basert på synlig fremføring og utgruppering av fiendtlige styrker, er i liten grad mulig i cyberdomenet. Egne forsvarstiltak må dermed baseres på antagelser om fiendens målsettinger, taktiske tilnærming og valg av angrepspunkt. Cyberdomenets størrelse og vekst medfører samtidig at begrensede cyberforsvarsressurser fortløpende må prioriteres dit de antas å ha størst effekt for egne operasjoner. Tilgangen til etterretninger spiller her en viktig rolle for å sikre at egne vurderinger er basert på så god informasjon som mulig.

Selv om egen etterretning bidrar til forutsigbarhet, vil kontinuerlig overvåking av infrastrukturen være nødvendig for å kunne stadfeste angrep og beskytte systemene effektivt. Gjennom analyse av data om fiendens rekognosering og taktiske tilnærming vil forsvareren kunne danne seg et bilde av hans målsettinger og strukturen i et pågående eller fremtidig angrep. Den offensive part vil tilsvarende være interessert i å kartlegge hvilke forsvarstiltak motstanderen kan aktivere. Aggressiv rekognosering som man antar motparten vil oppdage, vil i så måte være et mulig virkemiddel. Gjennom å fremprovosere forsvarsreaksjoner, kan angriperen få innsikt i forsvarerens kapasiteter og prosedyrer.

Cyberovervåking vil her spille en viktig rolle ved å muliggjøre tidlig indikasjon på angrep. Stadfesting av fiendens angrepspunkt, mål og metoder vil være sentrale elementer i en slik ambisjon. I tillegg vil cyberovervåking kunne bidra til å avgjøre om driftsforstyrrelser skyldes tekniske feil eller angrep. En strategisk defensiv cyberambisjon vil derfor være avhengig av den varsling og situasjonsforståelse som cyberovervåking gir.

Cyberangrep

Effekt av cyberangrep avgjøres ikke først og fremst av hvor stor funksjonssvikt de forårsaker i motstanderens datasystemer. Muligheten til å følge opp med nye operasjoner og angrepets psykologiske effekt er derimot viktigere. For å være effektiv må en taktisk suksess derfor skape resultater eller muligheter som er større enn de ødeleggelser som oppstår direkte. Den offensive cybertaktikkens natur er i så måte indirekte. Forskyvning og avgjørelse er avhengig av at man rammer motstanderens virksomhetsprosesser. Cyberteknikker som forstyrrer fiendens kognitive virksomhetsprosesser vil kunne frata ham situasjonsoversikten og villede soldatene. Tilsvarende vil angrep på datamaskinstyrte virksomhetsprosesser kunne øde-

legge eller forstyrre fiendens våpensystemer. Hensikten vil være å skape en stadig økende ubalanse i fiendens disposisjoner og derigjennom frata ham troen på egne planer og ressurser.

Angrep på IKT-systemer forutsetter at man omgår motstanderens forsvarstiltak. Elementet av overraskelse er her sentralt, både for å forhindre at fienden rekker å forberede sperretiltak og for å forsterke den psykologiske effekten av angrepet. Identifikasjon og utnyttelse av svakt beskyttede deler av fiendens systemer er en forutsetning for å skape overraskelse. I fysisk krigføring omgås fiendens sterke kapasiteter ved å manøvrere egne avdelinger til en fordelaktig posisjon, hvorfra man kan ramme hans kritiske sårbarheter. I cyberdomenet gjennomføres derimot ikke manøver ved å forflytte fysiske styrker, men ved å endre angrepspunktet. Informasjonsinfrastrukturen er normalt tilrettelagt for å gi optimal tilgjengelighet til ressurser og funksjoner. Mobiliteten i cyberdomenet er derfor potensielt stor. På den annen side gir ikke alle angrepspunkter tilsvarende tilgang til systemet. Grundig rekognosering og skreddersydde angrepsmetoder kan derfor i mange situasjoner være en forutsetning for å lykkes.

Cyberlendets uoversiktlighet og dynamiske struktur tilsier samtidig at effekten av offensive operasjoner kan være vanskelig å predikere. Kompleksiteten medfører at det ikke er enkelt å konstruere feilfrie cybervåpen. Selv små konstruksjonsfeil vil kunne medføre at cybervåpen ikke får virkning i målet eller skaper utilsiktet skade. Levetiden og reproduserbarheten til ulike cybervåpen kan dessuten medføre at de spres og aktiveres utenfor de krigførende parters kontroll.

Hensikten med cyberangrep er ikke primært å ødelegge fiendens systemer, men å frata ham troen på egne planer og kapasiteter. Forstyrrelser og ødeleggelser vil i så måte bidra til å bringe fienden ut av likevekt og derigjennom svekke hans vilje til å fortsette sine operasjoner. Samordnede angrep, i flere stridsdomener, vil dermed kunne ha en stadig økende effekt.

Konklusjon

Cyberdomenet er ikke lenger bare en arena for sosiale aktiviteter, økonomisk virksomhet, kulturutveksling og politisk innflytelse, men utgjør også et nytt område for militær makt. Militære operasjoner blir dermed vevd inn i det sivile samfunnets virksomhet, ut over de geografiske områder hvor konfliktene utkjempes.

Cyberdomenets verdensomspennende utbredelse har i seg selv medført endringer i trusselbildet. Dette er endringer som trolig vil øke i omfang i takt med teknologiens samfunnsmessige betydning. En synlig konsekvens er at cyberdomenet allerede er tatt i bruk som stridsarena. Forsvaret står dermed overfor en situasjon hvor egne høyteknologiske

våpenplattformer vil være attraktive mål for cyberangrep. Intelligente aggressorer vil relativt enkelt omgå forebyggende sikkerhetstiltak. En ren defensiv tilnærming til å beskytte Forsvarets IKT-systemer vil derfor ikke være tilstrekkelig. Vi kan derimot anta at evnen til å ramme en fremtidig fiendes datasystemer vil være en sentral forutsetning for å opprettholde egen kampkraft.

Militære operasjoner i cyberdomenet vil på flere måter skille seg fra operasjoner i de fysiske domenene. For det første er betydningen av tid og rom av underordnet karakter i cyberdomenet. For det andre skapes de fysiske effektene av cyberteknikker indirekte. For det tredje kan cyberteknikker som manipulerer informasjon direkte forstyrre fiendens situasjonsforståelse og evne til å utøve kommando og kontroll. I forhold til militære aktiviteter i sjø-, luft- og landdomenet fremstår dermed cyberteknikker både som utfyllende og alternative maktmidler. Potensialet for synergieffekter gjennom å integrere land-, sjø- og luftkomponentene i en felles informasjonsinfrastruktur og samtidig ramme fienden i cyberdomenet er betydelig. Ved planlegging av operasjoner og kampanjer bør derfor cyberoperasjoner samordnes tett med land-, sjø- og luftoperasjonene.

Cyberkapasiteter vil helt klart kunne tilføre Forsvaret økt operativ evne. Forutsetningen ligger derimot i hvorvidt Forsvaret endres i tilstrekkelig grad til å utnytte den nye teknologiens potensial. Gamle operasjonskonsepter blir ikke nødvendigvis bedre gjennom innføring av IKT. Et større fokus på situasjonsbevisstheten og samarbeidets betydning for militær effekt vil ikke bare påvirke Forsvarets IKT-investeringer, men i høyeste grad også organiseringen av militærmakten.

Litteratur

Alberts, David, John Garstka, Richard Hayes & David Signori (2001) *Understanding information age warfare*. CCRP.

Al-Jazeera (2012) Taking power through technology in the Arab spring. 26.10. Tilgjengelig på: http://www.aljazeera.com/indepth/opinion/2012/09/20129191153442998 48.html. Lesedato 27.12.2012.

Clausewitz, Carl von (1832) *On War*. Oversatt av Michael Howard & Peter Paret (1976). Princeton, New Jersey: Princeton University Press.

CNN (2011) Cyberwar explodes in Syria. 22.11. Tilgjengelig på: http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html. Lesedato 06.01.2013.

Denning, Peter J. & Tim Bell (2012) The Information Paradox. *American Scientist, 100* (6): 470–477.

Fuller, John Fredrick Charles (1932) *The Dragon´s Teeth*. London: Constable.

Helpern, J. & M. Tuttle (1993) Knowledge, probability, and adversaries. *Journal of the Association for Computing Machinery, 40* (4): 917–960.

Jones, A. & D. Ashenden (2005) *Risk management for computer security*. Oxford: Elsevier Butterworth-Heinemann.

Lewis, James A. (2011) Cyberwar Thresholds and Effects. *IEEE security and privacy, 9* (5): 23–29.

Parks, Raymond & David Duggan (2011) Principles of Cyberwarfare. *IEEE Security and Privacy, 9* (5): 30–35.

Ruge, Otto (1946) *Annen verdenskrig*. Oslo: Halvorsen & Larsen forlag.

Sabbagh, Karim et al. (2012) Maximizing the Impact of Digitization. I Soumitra Dutta & Benat Bilbao-Osorio (red.) *The Global Information Technology Report 2012*. Geneva: World Economic Forum.

Skar, Rune (2006) *Systemdynamisk tilnærming for risikoanalyse av transformasjonen til NbF*. Gjøvik: Høgskolen i Gjøvik.