Nu är det väl revolution på gång?

Teknologi, innovation, doktrin och den svenska armén

av Magnus Christiansson

Résumé

The article argues that multi-domain operations (MDO) — adopted as a NATO concept in 2023 with an implementation target of 2030 — are not a military paradigm shift but the latest version of a recurring idea of network-based warfare, similar to the Swedish NBF at the turn of the century, which failed. The driving force is global power politics: technological levelling (AI, drones, quantum technology) threatens Western military superiority, and the core of the battlefield is now data management in an electromagnetically vulnerable network — something that the war in Ukraine confirms in practice. The central warning is that Sweden risks repeating the NBF fiasco if MDO is not linked to strategic realities and organisational change. The conclusion is that the Armed Forces must build both a battlefield network and an innovation network — and that the ability to organise and adapt is more important than individual weapon systems or doctrinal abbreviations.

EN BÄRANDE DEL av arbetet för personalen vid den svenska Nato-representationen i Bryssel gäller implementeringen av alliansens strategiska koncept (SC 2022) och multidomänoperationer (*Multi-Domain Operations*, MDO).[1] Sedan mars 2023 är MDO ett koncept antaget av alliansen, och siktet är inställt på implementering till 2030.[2] Förkortningen är med andra ord inte bara en krydda i konceptpresentationer, utan också en integrerad del av Försvarsmaktens verksamhet och verklighet: om ett ledningsstödsystem inte kan dela lägesbild eller ta emot en order från en stab i den integrerade kommandostrukturen, är det inte operativt relevant.

Varför multidomänoperationer?

Tre huvudskäl till att MDO behöver tas på allvar kan identifieras. Dels i) eftersom Sveriges strategiska idé bygger på operationer inom ramen för Nato[3], dels ii) eftersom den gällande svenska doktrinen för gemensamma operationer (DGO 2020) inte erbjuder något tydligt alternativ och iii) eftersom utvecklingen av kriget i Ukraina kan ha konsekvenser för såväl DGO som MDO.[4]

Men trots att MDO är ett återkommande verksamhetsbegrepp (både strategiskt och operativt), är det mer sällan den svenska försvarsledningen utvecklar sina tankar om det, och det gäller i än högre utsträckning Sveriges politiska ledning.[5] Denna artikel syftar därför till att presentera ny och relevant forskning i ämnet, främst riktat till beslutsfattare i Försvarsmakten. I framställningen sätter jag drivkrafterna bakom MDO i strategiskt perspektiv, belyser några av huvuddragen i hur konceptet kan implementeras, samt skissar några tankar om hur implementeringen kan förbättras.

Jag tänkte inledningsvis göra det enkelt för mig när det gäller det centrala begreppet ”domän”. Multidomänoperationer handlar om operationer som samtidigt sker i flera dimensioner. Enligt Nato:s sätt att betrakta saken är mark, sjö, luft, cyber och rymd ”domäner”, vilket även är förenligt med två analytikers inklusiva definition:

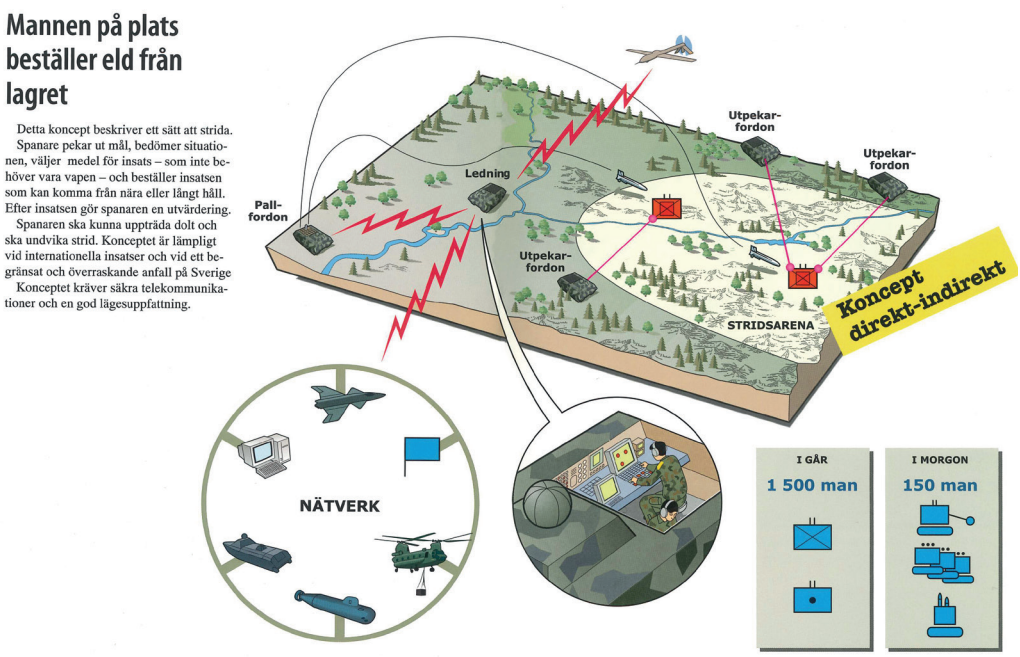
> Den inflytelsesfär inom vilken aktiviteter, funktioner och operationer genomförs för att lösa uppgifter och utöva kontroll över en motståndare i syfte att uppnå önskade effekter.[6]

Vidare använder jag som noterats den lite hemsnickrade översättningen “multidomänoperationer”, vilken trots allt är ett lite behändigare sätt att beskriva ”operationer i fler än en domän”. I rapportens slutdel kommer jag dock att återkomma till och problematisera domänbegreppet.

Vad är problemet?

Rapporten drivs av en forskningsgåta: *Hur skall vi förstå att nätverkskoncept inom operationskonsten tycks återkomma, och vilka slutsatser kan vi dra av det?* Frågeställningen kan övergripande illustreras av två populariserade konceptbilder som är publicerade med nästan 20 års mellanrum, *Figur 1* ”Total koll på läget”[7] och *Figur 2* ”Achieving cross-domain synergy”[8].

Dessa bilder har många gemensamma drag: de föreställer ett relativt glest stridsfält där ett nätverk av olika typer av förband knyts ihop av sensorer. I själva verket är likheterna över två decennier slående: färre traditionella manöverförband, bekämpning från luften och med långräckviddiga system. En

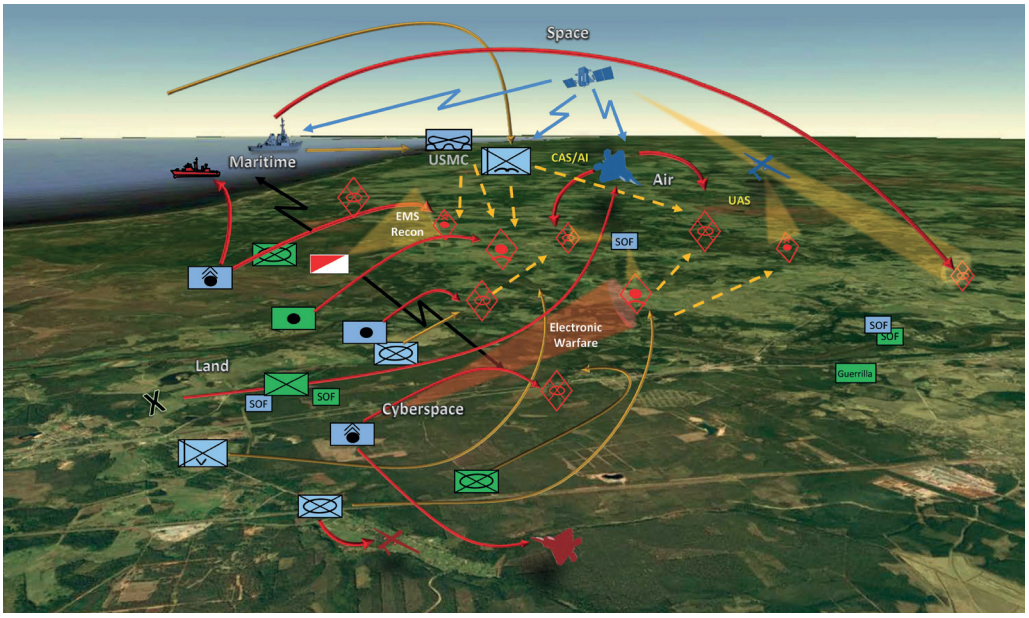


Figur 1 "*Koncept direkt-indirekt*".

traditionalist skulle kanske påpeka att de är goda exempel på den kavalkad av tidigare ”modeflugor” inom försvarssektorn som på många sätt skadat det svenska försvarets förmåga. Runt sekelskiftet 2000 kom en ”revolution i militära frågor” (RMA) att dominera militär doktrin. Med tekniska lösningar i centrum skulle slagfältets dimma skingras, och befälhavare skulle kunna följa varandra i detalj.[9] De tekniska möjligheterna att koppla samman verkansdelar skulle göra slagfältet mer utspritt och framgång i strid skulle bero på förmåga att snabbt koppla data om motståndarens gruppering till verkansdelar (*Dominant Battlespace Awareness*, DBA), oavsett om dessa fanns till lands, till sjöss eller i luften.

Eftersom det inte spelade någon roll i vilken domän verkansdelarna befann sig i nätverket, så skulle Försvarsmakten utvecklas mot att bli försvarsmaktsgemensamt (*joint*) och interoperabelt (samordningskompatibelt). Inom Nato utvecklades konceptet om nätverksbaserade kapaciteter (*NATO Networked Enabled Capabilities*, NNEC), och samma tanke återkom i Sverige från 2001 i ”nätverksbaserat försvar” (NBF). Några år senare kom det sistnämnda att flankeras av effektbaserade operationer (*Effect-Based Approach to Operations*, EBAO). Därefter följde Nato:s FMN (*Federated Mission Networking*), vilket den svenska doktrinen om gemensamma operationer (DGO 2020) stödjer sig på. Doktrinen om multidomänoperationer har utarbetades i övergången från det globala Västs övergång från expeditionära militära operationer, till förberedelser för att möta främst Kina och Ryssland i en militär konfrontation.[10]

Det är en god poäng att det finns risker med allt för framträdande plats för teknologidrivna *buzzwords*, vilka återkommande idisslas medan de göder en industri av analytiker på militära skolor och centra.[11] Traditionalister skulle invända att det är bättre att hålla fast och utveckla taktiska



Figur 2 ”Achieving cross-domain synergy”.

begrepp som hållit för tidens tand (så som uppdragstaktik).

Det stämmer också att NBF gick upp som en sol och föll ned som pannkaka, och i någon mening kom det nätverksbaserade försvaret att stå för allt som gick fel med den svenska Försvarsmakten runt sekelskiftet. Men givet att MDO är något som Sverige måste förhålla sig till behöver analysen också ta hänsyn till att liknande föreställningar om operationsmiljön uppenbarligen också är *återkommande teman i samtida militärteori*, alldeles oavsett vilka buzzwords eller aktuella bokstavskombinationer som används för att beskriva dem. Man kan vifta bort ett enskilt koncept, men uppenbarligen återkommer idén om det glesa och nätverkskopplade slagfältet.

> *Det finns risker med allt för framträdande plats för teknologidrivna buzzwords.*

Men just eftersom NBF blev ett misslyckande skulle Försvarsmakten därför vinna på att, i sökandet efter hur organisationen skall ta sig an de nuvarande och framtida tekniska lösningarna, också förhålla sig kritiskt till operativa koncept som MDO. *Hur kan Försvarsmakten utveckla MDO i samklang med sina allierade, utan att konceptet reduceras till ännu en modefluga?*

Utgångspunkten för att diskutera denna forskningsgåta och de vidhängande doktrinutmaningarna, är att bryta med tendensen inom konceptutveckling (*Concept Development and Experimentation*, CD&E) att koppla loss teknologi och krigföringen från ett strategiskt och politiskt sammanhang. Tvärt om behöver operativa förutsättningar knytas ihop med den strategiska miljön och dess politiska realiteter. Detta är med andra ord viktigt för att förstå *kontexten i vilket den återkommande fokuseringen på det glesa slagfältet och dess nätverk drivs och i vilket MDO endast utgör en variant*.

Upplägget i artikelns fortsättning har tre delar: i den första sätter jag in teknikutvecklingen i just ett strategiskt och operativt sammanhang; i det andra diskuterar jag knäckfrågan om hur och var domäner skall integreras organisatoriskt; och slutligen diskuterar jag hur Försvarsmakten (och speciellt armén) undviker att implementeringen av MDO misslyckas på samma sätt som vid införandet av NBF.

Multidomänoperationer i strategiskt och operativt sammanhang

Den strategiska miljön under perioden efter det kalla krigets slut har präglats av framväxten av vad den amerikanske statsvetaren Samuel Huntington kallat ”den ensamma supermakten”.[12] Det första kvartsseklet efter Berlinmurens fall innebar en triumf för globaliseringen (definierad som globala flöden av kapital, information, människor och varor), vilket resulterade i en oöverträffad period i mänsklighetens historia vad gäller ekonomisk tillväxt, välståndsökningar och sammankoppling av världens regioner. En effekt av detta är att den tidigare ”utvecklingsvärlden” idag i hög utsträckning blivit välståndssamhällen. Det innebär också att det globala Väst (löst definierat som det traditionella OECD-området) helt logiskt blivit en mindre andel av världsekonomin. I sin tur innebär detta att såväl *ekonomisk som militär makt blivit mer distribuerad i det internationella systemets aktörsnivå*, än vad som var fallet vid Berlinmurens fall 1989.

Huntington skrev sin text om den ensamma supermakten vid tidpunkten för framväxten av NBF, men den syftade framåt mot framtidens internationella system. Det system Huntington tecknade var ”uni-mul-

tipolärt", en märklig hybrid av hegemoni och stormaktskonkurrens (multipolaritet). Supermaktens främsta utmanare är Kina, Ryssland och Iran. Å ena sidan är USA fortsatt den i särklass största och mäktigaste staten (ekonomiskt, politiskt, militärt och kulturellt), men landet kan eller vill inte längre kontrollera världens institutioner och stå som garant för det som lite vagt brukar betecknas som "den regelbaserade världsordningen". USA är störst och viktigast, men inte överallt och inte hela tiden.

Denna strukturella förändring ligger också till grund för fyra megatrender, d v s sociala och politiska förändringar med globala konsekvenser.[13] Dels har den medfört enorma demografiska och sociala förändringar, där utvecklingsländer närmat sig de mogna välfärdsstaternas *demografiska förhållanden*. Det har till konsekvens att världen numera är *en värld av städer*, i en historiskt snabb urbanisering (och i redan industrialiserade länder, metropolisering). Utvecklingen har också resulterat i en *ekologisk katastrof* i form av mycket snabba klimatförändringar med potentiellt oöverskådliga konsekvenser för liv på planeten.

Slutligen har det också lett till en relativ *nivellering av teknologiska genombrott och innovationer.* Det gäller särskilt det som brukar kallas framväxande, omstörtande teknologier (*Emerging Disruptive Technologies*, EDT). Det kännetecknande för EDT är att de utvecklas i snabb takt, en "stormvind" för att använda ett begrepp av Robert Dalsjö[14], men att det saknas fullständig kunskap om deras effekter på samhället och deras potential att omkullkasta och förändra sociala system i grunden. De kanske mest omtalade gäller artificiell intelligens (AI), maskininlärning (ML), *Big Data Management* och *Internet of Things* (IoT). I en värld med en ensam supermakt har de regionala makterna börjat utveckla doktriner för användningen av EDT, vilka utmanar det globala Väst.

Men den teknologiska nivelleringen kanaliseras inte främst genom statsbudgetar. I stället är den privata sektorn ledande, inte minst mindre entreprenörer (*start ups*) med ofta svag koppling till försvarssektorn. Exempelvis ökade amerikanska försvarsdepartementet sin satsning inom forskning och utveckling från drygt 70 miljarder dollar 2016, till drygt 105 miljarder dollar 2020 (distribuerat på hundratals projekt)[15], och en ökning till drygt 118 miljarder dollar 2022.[16] Som jämförelse har endast en kvartett av de amerikanska techjättarna (Meta, Microsoft, Amazon, Alphabet) under 2025 spenderat 155 miljarder dollar bara på utvecklingen av AI (Montgomery, 2025). Det här är en värld av snabbt växande techföretag (företag med försvarskoppling inkluderar Anduril, Palantir, Helsing), vilka alla befinner sig i korsningen mellan stormaktpolitisk konkurrens, teknologisk innovation och framväxande system av nätverksstyrning (*governance*).

Denna utveckling är uppenbar inom AI-området. USA har en tätplats, men närmast efter följer Kina. När det gäller AI är det viktigt att skilja på "smala" och "breda" AI-system, där det senare attraherar mycket spekulation och det förstnämnda mer konkret innovation: exempelvis övervakning, logistik, automatiserade fordon. AI påverkar redan det offentliga samtalet, politiska partier och människors vardagsliv. Stort fokus ligger också på olika militära applikationer, allt ifrån autonoma system till beslutsstöd (mer om detta i rapportens nästa del).

Bioteknik, d v s teknologier som förändrar biologiska system, genomgår också en liknande förändring. Bioteknik öppnar bland annat upp för genmodifieringar av växter, djur och människor. Spridandet av syntetisk biologi som används för att skapa genetisk kod i naturen, kan öka antalet aktörer som

kan tillverka kemiska och biologiska vapen, adaptivt kamouflage samt kropps- och fordonspansar. Biometri, särskilt i kombination med Big Data Management, kan potentiellt leda till en revolutionerande effekt att all möjlighet till anonymitet för individen i samhället försvinner. Detta är något som redan finns på plats i Kina.

> *Nivelleringen av teknologi hotar USA:s militära överlägsenhet*

Rymdteknik är ytterligare ett exempel. Både Ryssland och Kina har rymdprogram. Kina har dessutom skjutit upp satelliter åt Algeriet, Argentina, Belarus, Bolivia, Ecuador, Egypten, Etiopien, Indonesien, Laos, Nigeria, Oman, Pakistan, Saudiarabien, Sudan och Venezuela. Våra samhällen är i hög utsträckning beroende av satelliter. Militärt används de för att samla in underrättelser, möjliggöra kommunikation och navigation, samt identifiera mål. Rymden är även en domän som snabbt militariseras, inte minst gällande sin roll inom kärnvapenavskräckning.[17] Även Sverige har höga ambitioner i rymddomänen.

En teknik som kan verka som motmedel är kvantumteknologi (kvantavkänning, kvantdatorer, och kvantkommunikation). Denna kan användas för att potentiellt bygga system med enorm beräkningsförmåga och bland annat göra det möjlig att navigera i en värld utan satellitpositioneringssystem (GPS).

Det pågår också en global utveckling av obemannade farkoster (ROV/UAS/UAV/UCAV/UUV), inklusive dödliga autonoma vapensystem (LAWS), populärt kallade ”drönare”. Mellan åren 2009 och 2019 ökade antalet länder som förfogar över tunga drönare (lämpliga för beväpning) från 11 till 30.[18] Exempel på välkända drönarmodeller inkluderar *Kronstadt Orion* (Ryssland), *Shahed-136* (Iran) och *Feihong* FH-97A och *Hongdu* GJ-11 (Kina). Framtidens drönarutveckling siktar mot större system (vätedrivna, sjusitsiga modeller på upp till tre ton i vikt, med förmåga till vertikal start och landning), flygplansliknande modeller med transportförmåga, hypersoniska drönare (Lockheed Martin SR-72), smygdrönare (*Northrop Grumman* RQ-180 och *Boeing Australias* MQ-28 *Ghost Bat*), såväl som mikroskopiskt små varianter. Utvecklingen av LAWS är både snabb och närvarande hos alla stormakter. Ett LAWS kan med algoritmer och sensorsviter identifiera, klassificera och destruera ett mål utan direkt mänsklig inblandning. Inom samma område pågår utveckling av olika tekniker för antidrönarkrigföring (ADW).

Hypersoniska vapen (HGV/HCM), d v s vapen med en hastighet över Mach 5, utvecklas i ett flertal länder (USA, Ryssland, Kina, Frankrike, Australien, Indien, Tyskland, Japan). Det finns även en hel räcka av nya system inom fältet direktenergi- och mikrovågsvapen (DE/HPM), Dessa innefattar såväl stråle- och värmevapen, populärt kallade ”lasrar”, vilka kan användas i såväl luftförsvar som repressivt gentemot politiska demonstranter.

Den ensamma supermaktens respons

Det finns med andra ord en militärstrategisk utmaning för USA som direkt följer av att det internationella systemet utvecklades ”uni-multipolärt”. Nivelleringen av teknologi hotar USA:s militära överlägsenhet i internationell politik. En australiensisk ranking bedömde 2023 att Kina är ledande inom 37 av 44 EDT.[19] Denna utveckling har tydligt påverkat USA:s doktrinutveckling.[20] Redan i styrdokumentet QDR (*Quadrennial Defense Review*) från 2014 reducerades den amerikanska militära ambitionen globalt till att ”besegra en regional motståndare i ett

storskaligt fälttåg i flera faser, och förneka målen – eller påföra oacceptabla kostnader – för en annan angripare i en annan region".[21] Med andra ord erkänner supermakten att man inte har kapacitet att besegra två motståndare i fälttåg samtidigt.

USA har också utvecklat två operativa ramverk i skuggan av denna utveckling. Dels förmåga att på distans bekämpa systemhotande terrorism (*networking*), dels förberedelser för en situation där landet behöver ta sig in i ett operationsområde (*access*), vilket försvaras av kvalificerade långräckviddiga system, så kallade A2/AD system (i det ryska fallet exempelvis S-400, *Bastion* och *Iskander*). I båda dessa ramverk är partners och allierade nödvändiga beståndsdelar. Vidare gör det uni-multipolära systemet också att det fortsatt framstår logiskt för USA att fokusera på strategier för att utveckla överlägsen teknologi som kan *kompensera för förlusten av hegemoni*.[22] Det finns dock tre utmaningar för utvecklandet av en samtida kompensationsstrategi. För det *första* att den inneboende dynamiken i den teknologiska utvecklingen (Moores lag, d v s att antalet transistorer på en integrerad krets fördubblas på två år) och det faktum att cyberteknologi, bioteknologi, DE/HPM, HGV/HCM, AI, IoT och ML utvecklas på så många ställen i det internationella systemet, och att utvecklingen går långt bortom supermaktens förmåga att förutsäga deras effekter. Systemet visar tecken på *emergenta effekter*, d v s nya och oväntade mönster kan uppstå, vilka i sig inte kan hänföras till de ingående delarna. För det *andra* att civil och militär teknik blir allt svårare att separera från varandra. Den teknologiska utvecklingen rymmer oftast både civila och militära applikationer. För det *tredje* att den teknologiska utvecklingen är präglad av komplicerade nätverk av både militära och civila aktörer. Staten och de etablerade försvarsföretagen är ofta inte de ledande inom EDT.

Oförmåga att förutsäga effekterna av den teknologiska utvecklingen och statens oförmåga att ensam kontrollera teknikutvecklingen, driver därför en *innovation av teknikinnovationen*. Det är i själva verket detta som är kärnan i den "tredje kompensationsstrategin" (*3rd offset strategy*).[23] Den handlar i grunden om att *organiseringen* av den tekniska utvecklingen måste utvecklas, d v s att det i sig inte handlar om vilka vapensystem som utvecklas, utan om *hur* vapensystemen utvecklas. Statens uppgift i denna nätverksstyrning är att skapa arenor och mötesplatser för intressenter i försvarsinnovation (entreprenörer, industri, militären och politiker). Poängen är att snarare ha ett bättre innovationssystem än de regionala utmanarstaterna (Kina, Ryssland och Iran), än att fokusera på innovationsprojekt som skall identifieras, kravsättas och utvecklas från statens sida. Det är dock viktigt att tänka på att *behovet* av en kompensationsstrategi inte är det samma som att den nödvändigtvis är genomförbar i praktiken.[24] I detta sammanhang är det noterbart att även Sverige går en liknande väg med Regeringens försvarsinnovationsinitiativ. Under 2024 fick Försvarsinnovationsrådet uppgiften att samverka mellan den civila sektorn och Försvarsmakten, i syfte att hantera försvarsrelaterade problem. Alla dessa initiativ till trots kvarstår ett trevande sökande för hur det globala Väst skall försöka utnyttja sina innovationssystem som en fördel i en tilltagande global konkurrens.

Slagfältet: autonomi, transparens och sårbara nätverk

Poängen med framställningen hittills är att det således är *global maktpolitik (via sina konsekvenser för ekonomi och teknik) som driver frågan om hur Väst skall hantera*

dagens och morgondagens operationsmiljö. Operationsmiljön präglar dagens och morgondagens slagfält (*battlespace*). Ett exempel är hur utvecklingen av drönare i Ukrainakriget upplöser skillnaden mellan kryssningsmissilen och envägsattackerande drönare (OWA UAS).[25] Den lägre kostnaden och ökade precisionen har förskjutit tyngdpunkten från artilleribekämpning, vilket skapat ett behov av att såväl drönare som motmedel (CUAS), inklusive DE/HPM, i samtliga försvarsgrenar.[26] Med andra ord formas slagfältet just av de teknologiska områden som blivit mer nivellerade i det internationella systemet, och som också speglas i att de traditionella domänerna mark, sjö, luft i MDO har fått sällskap av också cyber och rymd.

Nätverkskaraktären som uppstår som en konsekvens av den tekniska utvecklingen, innebär att stridens grundläggande krav på förbanden är *insamling, utbyte, distribution och lagring av data*. Begreppet ”data” skall i det här sammanhanget läsas som ”information insamlad för användning”. Nätverket är den ”digitala ryggraden” för förbandens verkansdelar och de tenderar att bli mer beroende av digitala kommunikations- och informationssystem (CIS). En återkommande poäng i studier av det samtida slagfältet är att ett förbands värde på slagfältet i hög utsträckning beror på dess utökade förmåga till datahantering. Invigningen i september 2025 av den franska arméns superdator *Amiad* är möjligen ett tecken på att denna process blir alltmer konkret.[27] Vidare gör den stadigvarande övervakningen från rymden med satellitkommunikationsteknik att tillgången på data om slagfältet ökar betydligt.[28]

Det går också att betrakta drivkraften för det glesa slagfältet som en konsekvens av att armén söker undvika indirekt eld. Ledningsplatser är lättare att upptäcka och deras ökade betydelse för hantering av data på slagfältet gör dem samtidigt svårare att gömma för fienden. Ledningsplatser syns på grund av logistiken, värmesignatur, digital signatur och elektromagnetisk strålning. Med krigets inneboende dynamik blir kontroll, skydd och dominans av data en nödvändighet.

Det elektromagnetiska spektret (EMS) är grunden för insamling, utbyte, distribution och lagring av data. Det innebär att EMS och krigföring i det elektromagnetiska spektret (*electromagnetic warfare*, EW) följer som en del av kriget. Om en motståndare attackerar eller manipulerar användningen av radiofrekvenser med elektromagnetiska störningar (EMI, *jamming* och *spoofing*), skulle denne kunna förhindra åtkomst till viktiga satelliter som Nato och USA är beroende av för underrättelsetjänst, övervakning och spaning, kommunikation, förvarning, och navigering. Erfarenheten från Ukraina är att störningar och påverkan sker kontinuerligt, men att det samtidigt är svårt att helt förneka fienden tillgång till EMS. Att ha reservlagring av data, liksom etablerandet av stödfunktioner (*Cyber and Electromagnetic Activities Command*, CEMA) är grundläggande. I detta sammanhang är det viktigt att understryka hur användningen av mobiltelefoner och deras applikationer från den civila sektorn (*dual use*) har blivit helt centralt. Exempelvis använder ukrainarna mobilappen *Diia*, vilken i sig hyser appen *Delta* som möjliggör realtidsutbyte av taktiska data.[29]

En utmaning på det glesa slagfältet, vilken bekräftas av erfarenheterna i Ukraina, gäller förflyttning av förband. För det första gäller det vikten av snabb förflyttning. Den ständiga förekomsten av ISTAR (*Intelligence, Surveillance, Target Acqisition, and Reconnaissance*) och flera lager av sensorer, gör att fordon som färdas på den så kallade ”nollinjen” eller ”gråzonen” i Ukraina, har mycket kort överlevnadstid.

Det betyder dels att förflyttningarna måste vara snabba, dels att EW behöver användas för att tillåta en ökad koncentration av förband längs frontlinjen. Ytterligare en utmaning är problemen att skilja vän från fiende längs fronten, speciellt när förband gör samtidiga förflyttningar och echelongsbyten. I Ukraina har man i sådana situationer gjort sig synliga med hjälp av färgband, och helt förlitat sig på skydd i form av snabb förflyttning. Det har växt fram en intressant debatt om huruvida det transparenta slagfältet har gjort det svårare att anfalla.[30]

I alla händelser skulle konsekvenserna av omfattande fientliga EW attacker allvarligt begränsa en militär chef i planerings-, besluts- och genomförandecykeln och i värsta fall helt kullkasta en militär operation. Med andra ord, exempelvis ett tidigt ryskt eller kinesiskt angrepp i en konflikt kan komma att göra Västsidan, med en metafor, både blind och döv innan striderna ens börjat. Den kritiska sårbarheten på slagfältet innebär att förband kommer att verka i helt eller delvis störda elektromagnetiska miljöer (*degraded operational environment*), i vilka det pågår en kamp för domänöverlägsenhet (*domain superiority*).

En analys av den teknologiska utvecklingen i den tredje kompensationsstrategin ger därför vid handen att det, grovt räknat, finns två olika typer av EDT: dels system som inlemmas i mark, sjö och luftdomänerna (exempelvis förbättrade missilsystem), och dels system som förändrar operationerna i mark, sjö och luftdomänerna, och som därmed också blir en potentiell operativ sårbarhet för dessa (exempelvis satelliter och cyber). Den operativa miljön lägger med andra ord till *ytterligare dimensioner* till de etablerade domänerna mark, sjö och luft. En vanlig slutsats är därför att *joint* inte är tillräckligt[31] – framgång för exempelvis markstridskrafterna bygger på stöd från inte bara sjö och luft, utan också tillgång till rymden och det elektromagnetiska spektret. Men denna förändring är än mer genomgripande än bara en förbättring av domänerna: armén, marinen och flygvapnet kan inte agera operativt vid sidan av dessa dimensioner (exempelvis för tillgång till måldata) och verkansplattformar är beroende av cyber och rymd för att åtminstone delvis ha domänöverlägsenhet. Att skydda nätverket är integrerad med försvarsgrenarnas uppgift.

Sveriges nuvarande doktrin DGO 2020 utgår från denna realitet, vad chefen för Sveriges operationsledning kallat ”det digitaliserade kriget”[32], då den som vi tidigare konstaterat talar om ”integrationstänkande”. Att integrera domäner innebär på ett övergripande plan att betrakta operationsmiljön i ett holistiskt snarare än ett försvarsgrensperspektiv. I DGO 2020 illustreras detta med ett grått moln som svävar runt ”svensk operationskonst”.[33] Men vad innebär detta mer konkret? I DGO 2020 är dessa faktorer svävande (”synergier genom integrering”), och utan att precisera vad dessa utmaningar innebär riskerar viktiga beståndsdelar för nätverket att bli oanvända, dåligt koordinerade eller ineffektiva. Givet den föregående diskussionen tror jag att det finns tre huvudsakliga utmaningar: hantering av potentialen för autonoma system, semi-transparens på slagfältet, samt sårbarheten i slagfältets nätverk. Den operativa miljön är, åtminstone utifrån doktrinperspektivet, helt enkelt så full av elektroniska apparater att EMI är ett mycket stort hot mot hela operationsplanen. Så hur skall ”integrationstänkande” gå till?

Multidomänintegration

I artikelns förra avsnitt diskuterades två faktorer: teknologi (huvudsakligen autonoma system, semi-transparens och sårbara nätverk

på slagfältet) och innovation (governance). I det följande diskuteras utvecklandet av doktrin, d v s hur teknologi och innovation kan domänintegreras. Detta är en oundviklig del i en diskussion om vilka slutsatser som kan dras av att nätverken tycks återkommande i den militärteoretiska debatten, men detta innebär självklart inte att ambitionen i det följande är att belysa alla tänkbara valmöjligheter. Doktrin ger svaret på avvägningar i valet av skyddsnivå (fåtal dyra, skyddade enheter eller många förbrukningsbara); teknikнivå (världsledande eller tillräckligt bra); relation mellan människa och maskin (HMI); avvägning mellan hierarki och nätverk; fokus på plattformar eller mjukvara; centraliserad eller förbandsnära utveckling och valet mellan fasta krav respektive iterativa krav i materieltillverkningen. I det följande kommer jag endast göra några observationer om dessa avvägningar.[34]

> *Innovation är en del av den militära verksamheten, inte något som kommer utifrån.*

Betraktad från ett strategiskt perspektiv är det nuvarande internationella systemet (Huntingtons uni-multipolaritet) ett emergent system, och just därför svårbedömt. Slagfältet består av nätverk, men det gäller också teknikutvecklingen. Detta påverkar i grunden hur militären som socialt system reproduceras: innovation är en del av den militära verksamheten, inte något som kommer utifrån. Föreställningen om MDO innebär alltså inte bara ett sätt att organisera sig på slagfältet, det innebär att bli en del av ett innovationsnätverk. Det är i detta strategiska sammanhang multidomänoperationer tillkom, som ett samutvecklat vitpapper mellan amerikanska armén och marinkåren i oktober 2016 (för övrigt samma år som Nato erkände cyberspace som en operationsdomän).

En av erfarenheterna från kriget i Ukraina är behovet av allierade i en utdragen konflikt, och Nato erbjuder flera möjligheter som politiskt nätverk. Inom försvarsplaneringsprocessen (NDPP) finns möjlighet till koordinering inom alliansen i syfte att harmonisera nationella planer och kapacitetsutveckling. De allierade kan göra en bedömning av vilka i medlemskretsen som skall utveckla nyckelteknik, speciellt gällande förmågemål (*Minimum Capability Requirement*) för situationer av acceptabel försämring (*graceful degradation*) av materiel. Nato kan utgöra en ”ledstjärna” (*NATO Warfighting Capstone Concept,* NWCC) för navigering mot framtiden, vilket inkluderar strävan mot kognitiv överlägsenhet, flerskiktad motståndskraft (*layered resilience*), domänintegrerad ledning (*cross-domain command*) och integrerat multidomänförsvar.

En av utmaningarna är att dra nytta av Västs innovationskraft inom EDT (exempelvis övervakningsteknik, cyber, rymd, elektromagnetiska förmågor). Förre chefen för ACT Philippe Lavigne har talat om behovet av “ett ekosystem där man runt bordet har de stora aktörerna från försvarsteknologi, men också mindre aktörer [från forskning och utveckling], universitetspengar och investeringsfonder”.[35] En strategisk lärdom från Ukraina är att organisering (d v s förmåga till utbildning, övning och planering) snarare än tekniken i sig, är avgörande. Detta betyder sannolikt att Västs militära organisering och ledning behöver utvecklas[36] för att förstå hur ny teknik kan förbättra existerande system (som exempel: hur mikrodrönare i Ukraina förkortat bekämpningstiden för artilleri).

Den ukrainska framgången 2022 tillskrivs ofta förmågan till anpassning (speciellt på taktisk nivå) och snabbt utvecklade kapa-

citeter och koncept. Den centrala frågan i detta sammanhang gäller förmågan för taktiska formationer att kunna upphandla och testa utrustning.[37] Upphandling är inte separerade från förbanden. Det är dessutom av strategisk vikt att en sådan organisation etableras innan kriget bryter ut, inte minst eftersom kriget i Ukraina lär oss att förberedelser för ett långt och utdraget krig är av stor betydelse.[38] Långa krig kräver ersättningsbara, kostnadseffektiva kapaciteter som kan fältanvändas snabbt.

Från ett operativt perspektiv är utmaningen att integrera fem domäner i en struktur med människor vars kognitiva horisont oftast sträcker sig till tre domäner. Med andra ord berör den relationen mellan teknik och människa på ett slagfält. Närmare definierat finns det tre drivkrafter: dels behovet att överleva för att ens kunna börja manövrera och slåss på slagfältet, dels behovet av domänöverlägsenhet och dels behovet av ”nya” former av överraskning. Eftersom krigföringen potentiellt är snabbare än människans förmåga att skapa situationsförståelse, finns ett dilemma mellan å ena sidan kravet på uppkoppling i nätverket och å andra sidan behovet av att försvinna från det elektromagnetiska fältet för att skydda sig.

Valet av hur relationen mellan människa och teknik skall se ut, beror i sin tur på hur relationen mellan data och beslutsfattande skall se ut. Slagfältets nätverk drivs av behovet av att dela data, det är dess kärna. Betydelsen av interoperabilitet är förmågan att dela data och på denna punkt finns en parallell till det civila begreppet ”data som service” (*data-as-a-service,* DaaS) där molntjänster utnyttjas för att hantera och bearbeta data i ett nätverk. Analogt med detta har dagens slagfält ett multidomänmoln eller slagfältsmoln (*multi domain combat cloud*). Det består oftast av data med olika grader av sekretess och utveckling av såväl rutiner och spridning liksom att mjukvaruutveckling kräver övning (vilket också praktiserats inom Nato sedan åtminstone *Steadfast Jazz 13*).

I nätverket krävs koordinering mellan medel som verkar i helt olika tidsperspektiv. Det är viktigt att ge beslutsfattare möjlighet att utnyttja hela ”verktygslådan” i nätverket och samtidigt få överblick över sårbarheter och möjligheter, samtidigt som det gäller att kunna slå till snabbt mot en fiende. Tekniken kan användas för att integrera olika datakällor (elektro-optiska, infraröda, radar, akustiska) från olika domäner. Det handlar med andra ord inte bara om delad lägesuppfattning, utan om hur beslut skall tas i operationer. Delvis pådrivande denna utveckling, delvis som en hjälp för att hantera mängden data, har HMI-baserade ledningsstöd börjat utvecklas. De möjliggör i bästa fall dynamisk målhantering (*dynamic targeting*) och datahantering i realtid (*dynamic synchronization*). Utvecklingen har drivits mot en situation där data från domänerna kopplas samman och där maskiner väger risk, sannolikheter, osäkerhetsfaktorer, komplexitet, konsekvenser och ansvar vid olika handlingsalternativ (*Human-In-The-Loop*, HITL, *Human-On-The-Loop*, HOTL respektive *Human-Out-Of-The-Loop*, HOOTL).

Flera analytiker understryker att det bör finnas en strävan efter mänskligt samtycke som utgångspunkt, inte att människan endast kommer in i undantagsfall. Det finns olika ansatser för att hantera den kognitiva processen för att skapa mänsklig situationsförståelse i en maskindriven process.[39] En modell som väckt intresse försöker bygga in rutiner för att också föra fram data som talar emot ett maskingivet alternativ, allt i syfte att låta uppgiften styra flödet av data i stället för tvärt om.

Dessa varianter av automatiserad verkanskedja är utgångspunkten för de ledningskoncept som både USA nationellt och

Nato utvecklar inom ramen för MDO. Som en spansk officer konstaterat är ännu de flesta operationer dock ”mono-domäna”.[40] Utmaningen för ledningsstödet är att övergå till stridscentrerad snarare än ledningscentrerad verksamhet, vilket innebär att besluten delegeras till chefer som har mandat och möjlighet att agera med förmågor i alla domäner. Vi kan notera att det inte finns någon egentlig skillnad på domäner och funktioner i dagens doktriner inom Nato, och att den stridscentrerade ambitionen inte i sig gör skillnad mellan civila och militära resurser.

Ursprungligen 2017–18 experimenterade USA med ett pilotprogram för övningar med stridsgrupper i *US Pacific Command*. Erfarenheterna från denna period var att skapa multidomänoperationscentra: antingen som en cell som stödjer mark-, sjö- och luft, eller en AI-lösning som använder hela stabens data (inklusive rymd- och cyberförmåga). En annan erfarenhet är att använda den delegeringsmöjlighet som redan finns inom Nato:s taktiska stridshanteringsfunktioner (TBMF) för att skapa taktiska multidomänfunktioner.[41] Erfarenhetsbanken har fyllts på av experimentverksamhet, interaktiva testbäddar, övningar, demonstratorer och krigsspel inom och utanför Nato:s ram.

Experimenten utgår ofta från den etablerade militära principen att fördela understödd/understödjande förband i enlighet med högre chefs bedömning (*supported/supporting interrelationship*, SSI). Förmågan att snabbt samordna data på slagfältet beror i hög utsträckning på utvecklingsgraden av tekniken inom tre dimensioner. För det första gäller det förmågan att *distribuera* data i nätverket (från ingen till omfattande), dels gäller det förmågan för enheterna i nätverket att *interagera* med varandra (från begränsade till obegränsade) och slutligen gäller det *beslutsrättigheter* för enheterna i nätverket (från begränsade till breda och allomfattande).[42]

Målet för denna verksamhet är att utveckla ett synkroniserat, motståndskraftigt och interoperabelt ledningsstöd som kombinerar dynamisk målhantering och datahantering i realtid. Denna idé om dynamisk ledning (*dynamic C2*) finns i Nato:s operationskoncept (*Joint All-Domain Operations*, JADO), såväl som AJP-6 (för CIS) som antogs 2024. Det amerikanska ledningskonceptet (*Joint All Domain Command, and Control*, JADC2), anger målet att skapa en modulär, skalbar och flexibel ledningsstruktur. I Nato:s ledningskoncept (*Cross Domain Command Concept*, CDCC) inriktas ledningsutvecklingen 2040 mot kollaborativ ledning (orkestrering och synkronisering). Det senare konceptet innefattar en vägkarta för implementering av nätverksledning med delmål: att förändra organisationen i SHAPE och fortsatt använda övningar för att experimentera med orkestrering och synkronisering av resurser som inte är underställda Nato:s ledningskedja. Implementeringen överses av en särskild grupp i SHAPE (*Strategic Initiatives Group*, SIG). Frågan är dock hur implementeringen skall gå till och hur den skall bli framgångsrik. Sverige kan med andra ord, likt många andra länder, konstatera att ”hur en allierad nation implementerar MDO inom sina försvarsgrenar, försvarsministerium och myndigheter är inte tydliggjort”.[43]

Reformutmaningar

Denna artikel har hittills skissat ett strategiskt sammanhang i vilket det nätverksbaserade slagfältet återkommit under de senaste decennierna. Den har även målat upp hur de nuvarande teknologiska realiteterna ser ut och hur alliansen hanterar dessa i sina doktriner. Givet den experimentella karaktären på implementeringen blir det av stor vikt att resonera kring hur Sverige och den svenska armén kan hantera MDO.

Det finns många likheter mellan dagens strategiska situation av reformering av stridskrafterna, och tidigare situationer i historien. Krigföringen utvecklades experimentellt under mellankrigstiden och senare närmast explosionsartat under 1940-talets krigsförhållanden. Det finns också många likheter med utvecklingen under 1970-talet, då det fanns stora förhoppningar om att ta ”ett stort kliv framåt” inom teknologisk utveckling och införandet av doktrinen *AirLand Battle*.

> *Det finns många skillnader mellan den nuvarande situationen och tidigare försök att bygga nätverksbaserade lösningar.*

Det är slående hur dagens situation med framväxten av ett nätverksbaserat slagfält (inklusive erfarenheterna från kriget i Ukraina) liknar framväxten av det nätverksbaserade försvaret runt sekelskiftet 2000. Det finns med andra ord en återkommande idé om att data driver slagfältet, att snabbt utnyttjande av data möjliggör framgångsrik bekämpning, vilket i sin tur möjliggör seger i ett krig. Det fanns redan i NNEC tankar om behovet att dela data (*Share to Win*) och ”system av system” på slagfältet. Samtidigt är det också påtagligt hur denna utveckling på intet sätt gjort många traditionella soldatfärdigheter otidsenliga.

Poängen med att uppmärksamma dessa kontinuiteter är att det är missvisande att tro att MDO utgör ”ett militärt paradigmskifte”.[44] Snarare är det den senaste versionen av en tanke som utvecklats successivt med tekniken under flera decennier. En gradvis utveckling från en plattforms- och typmaterielcentrerad Försvarsmakt till en alltmer mjukvarubaserad och innovationsfokuserad Försvarsmakt, förefaller vara en stark drivkraft. Poängen med detta konstaterande är att många av erfarenheterna från operationskonstens utveckling, inklusive gemensamma operationer, fortfarande är relevanta.

Samtidigt är det också tydligt att det finns många skillnader mellan den nuvarande situationen och tidigare försök att bygga nätverksbaserade lösningar. Dels har tekniken blivit mognare. Visionära plattformar har tagit klivet ut från Power Point-presentationerna på ett sätt de inte kunde runt sekelskiftet 2000 (en konsekvens av Moors lag). 5G-tekniken erbjuder hög och tekniskt pålitlig bandbredd. Utvecklingen av AI har snarare överträffat många prognoser från sekelskiftet, och till skillnad från NBF drivs utvecklingen i hög grad av civil teknik snarare än militär forskning och utveckling. Med hjälp av satelliter kan ledningsstödsystem fungera även om markbaserad infrastruktur är utslagen. Kriget i Ukraina visar att grunddragen i slagfältet som nätverk på ett semi-transparent slagfält existerar idag.

Det finns också en hel del träffsäker kritik mot MDO och tanken på multidomänintegration. Det är en återkommande kritik av nätverksbaserade koncept att fullständig integration varken är tekniskt, organisatoriskt eller kulturellt genomförbart.[45] Två analytiker pekar på begreppsförvirringen kring MDO, möjligen därför att förkortningen än så länge är positivt laddat och drar till sig uppmärksamhet från många aktörer inom försvarsorganisationerna. Det finns olika syn på vad som konstituerar en domän och inte minst hur begreppet skall organiseras praktiskt. I länder som USA, Storbritannien, Tyskland, Frankrike och Israel har uppgiften med domänintegration givits till markdivisionen.[46] I Nato pekas ofta armékåren ut som den ”kritiska echelongen i utförandet av MDO”.[47] CDCC utvecklar dock inga detaljer om vare sig orkestrering, synkronisering och AI. I brist på tydlighet finns dess-

utom risken att ledningsstöden blir så omfattande att mer fokus ligger på dessa än på att bekämpa fienden.[48]

Än mer problematiskt, vilket påpekats av Lawrence Freedman, är det flitigt förekommande grundantagandet att snabbt agerande på slagfältet innebär ett snabbt strategiskt avgörande av kriget.[49] Det komplicerade samspelet mellan taktisk och strategisk nivå har inte blivit mindre komplext med den tekniska utvecklingen. Möjligen är grunden i problemet att det finns en ontologisk utmaning att konceptualisera en verksamhet som rymmer både tids- och rumsgränser (mark, sjö, flyg) och sådana som förvisso har en rumsdimension, men som i sig är en del av funktionen i de andra (cyber och rymd).

> *Sverige måste skapa en ledningsstruktur som uppmuntrar innovation och snabb teknikintegration.*

Som tidigare konstaterats pressar den strategiska situationen i världspolitiken Väst att ligga främst i teknikutvecklingen. Det var således inte grundförutsättningen för det nätverksbaserade försvaret som de amerikanska pionjärerna fått om bakfoten runt sekelskiftet 2000. Det intressantaste är inte heller en skolastisk diskussion om för- och nackdelar med hur denna utveckling gör sig gällande i olika typer av koncept. Sverige kan välja hur man hanterar den återkommande teknikanpassningen, men inte låtsas att den inte gör sig gällande. Med andra ord har den tekniska utvecklingen varit successiv, men den kumulativa effekten har nu blivit disruptiv. Konsekvenserna innebär således att det finns behov för det svenska försvaret att genomgå ”en genomgripande förändring”.[50] Den stora frågan är snarare var och hur dessa nätverk skall organiseras i en nationell- och allianskontext.

Den datadrivna Försvarsmakten: beslutsstöd, doktrin, kulturell förändring

De mest omedelbara erfarenheterna av domänintegration har dragits från kriget i Ukraina. Med andra ord är det oundvikligt att följa denna utveckling, men poängen är inte att alla erfarenheter går att överföra till svenska förhållanden. Den svenska arméns experimentverksamhet på P7 har identifierat den svenska målsättningen som den ”datadrivna brigaden” vars ledning utgår från ”en distribuerad nätverksstruktur”.[51] Arméns experimentverksamhet rekommenderar att brigaden bör bygga upp en underrättelse- och understödsbataljon med förmåga att leda lägesbild, autonoma system och långräckviddig bekämpning.[52] Denna idé ligger också i linje med erfarenheter från kriget i Ukraina.[53]

Men frågan handlar inte bara om slagfältsnätverk (mark, sjö, luft). Det är en minst lika viktig dimension att forma ett innovationsnätverk (experiment, utveckling, anskaffning). På detta område formulerar sig P7s experimentverksamhet närmast desperat. Det anses tydligt att ”Sverige måste skapa en ledningsstruktur som uppmuntrar innovation och snabb teknikintegration, annars blir våra förband taktiskt förutsägbara och irrelevanta”.[54] Därför är det ”brådskande att integrera CD&E i ordinarie verksamhet”.[55] I praktiken är den svenska användningen av Systemmålsättningar (SMS) inte längre ändamålsenlig och ”därför måste en betydande del av anskaffningen ske direkt av brigaderna”.[56]

Behovet att kopplas till slagfälts- och innovationsnätverk finns inte bara för förbanden, utan också i lika hög grad för för-

svarsgrenarnas och Försvarsmaktens beslutsstöd. I Ukraina har förbanden, som ovan nämnts, involverats och drivit CD&E, men även Ministeriet för digital transformation har utvecklat flera intressanta utvecklingslinjer på strategisk nivå. Att djupare involvera försvarsgrenarna innebär en fortsatt organisationsutveckling i enlighet med logiken som redan pågått under decennier. Försvarsgrenarna behöver likt förbanden bygga nätverk mellan varandra, inte minst för att dela erfarenheter av att hantera frågor man aldrig hanterat förut.[57] Även försvarsgrenarna behöver bygga nätverk också till allierade och civila aktörer som det är särskilt viktigt att ha en relation till. Exempelvis behöver prestationerna av AI-genererade beslutsunderlag hela tiden utvärderas, och detta är ett typexempel på en funktion där det redan finns öppna och etablerade verktyg i den privata sektorn.[58]

Som konstateras ovan existerar mycket av den relevanta tekniken för slagfältet redan som civila applikationer, men på grund av kulturellt grundade föreställningar används de inte militärt.[59] Lösningar för framtiden innebär följaktligen kulturell utveckling och förändring: från behovet att skydda data till att dela data. Som historikern Michael Howard konstaterat är det egentligen inget problem att ha fel doktrin på plats när kriget börjar, eftersom det avgörande är förmågan att ”få den snabbt på plats i rätt ögonblick”.[60] Eftersom kampen i det uni-multipolära systemet har intensifierats, är det hög tid att öka takten i denna förändringsprocess. Hur snabbt tekniken än utvecklas kan den inte kompensera för behovet av människans anpassning.

Slutsatser: behovet av slagfältsnätverk och innovationsnätverk

Det är global maktpolitik som driver frågan om hur Väst skall hantera dagens och morgondagens operationsmiljö, nätverksslagfältet. Ett grundläggande antagande är att varianter av det glesa och nätverksbaserade slagfältet kommer att återkomma så länge det förhåller sig så.

Det underliggande antagandet för utvecklingen av slagfältet är att effektiv hantering av data leder till snabbare bekämpning, vilket i slutändan leder till framgång i kampen mot en fiende. Det finns i sig inget att invända mot resonemanget: på taktisk nivå finns det inget förband som vill bli bekämpad i en duellsituation, på operativ nivå finns det ingen fältherre som vill bli av med sina resurser, och på strategisk nivå finns ingen politiker som bejakar stora militära förluster. En viktig poäng med resonemanget om nätverksslagfältet är att det finns en begränsad vits att kritisera enskilda formuleringar i en doktrin eftersom den centrala utmaningen förefaller vara att förstå hur domänintegration skall organiseras. Snarare än en ändlös jakt på perfekta formuleringar i doktrindokument behövs regler och rutiner för hur nätverksbyggande skall ske på taktisk, operativ och strategisk nivå.[61] Det viktiga är inte MDO utan förändringarna i variablerna teknologi och doktrin.[62]

Militären är i sig själva en del av inte bara ett slagfältsnätverk (inomorganisatoriskt och med allierade), utan också ett innovationsnätverk (experiment, utveckling och anskaffning av EDT). Dessa nätverk kan delvis vara överlappande eftersom de konstitueras av en mer flytande uppbyggnad än en hierarki. Detta ligger också i linje med den politiska inriktningen för Försvarsmakten om snabbare reformering, och en förändrad syn på anskaffning och materielanskaffning.

Överbefälhavaren har en roll som övergripande ansvarig inom Försvarsmakten, inte minst för säkerhetsdimensionen i de system som byggs upp, men också internationellt gentemot allierade och kommersiella

aktörer på koncernivå. Här kan det strategiska beslutsstödet behöva utvecklas, så att Försvarsmaktens ledning kan fatta uppdaterade och informerade beslut baserade på teknikutvecklingen och den politiska inriktningen. Det är viktigt att börja tänka i termer av harmonisering, vilket gör att exempelvis allierade i Norden varken kan ligga för långt framme eller för långt efter i den tekniska eller organisatoriska utvecklingen. Försvarsgrenarna måste också få en aktivare roll och kan inte heller ha en utveckling som är isolerad från såväl allierade som den civila tekniken. *Tabell 1* illustrerar nätverksuppbyggnaden och fokus för olika nivåer i systemet:

	Slagfältsnätverk	Innovationsnätverk
Strategisk	Nato, Norden	DIANA, Nordefco
Operativ	Nato, Norden, Försvarsmakten	Försvars-innovationsrådet
Taktisk	Försvarsmakten, försvarsgren	Lokala

Tabell 1 Slagfältsnätverk och innovationsnätverk

Det finns en levande debatt om hur den teknologiska och organisatoriska utvecklingen påverkar kombinerade vapen, såväl stridens som förbandens karaktär.[63] Detta är en debatt som denna artikel av utrymmesskäl inte kan diskutera på djupet. En global nivellering av de ekonomiska och teknologiska förutsättningarna har också förutsättningen att nivellera möjligheterna till seger. Å andra sidan kan teknisk överlägsenhet leda till motåtgärder som syftar till att *dra ner tempot* på slagfältet. Att förbanden är integrerade i denna process gör det viktigt att öka förståelsen för hur innovation även kan *påverka motståndarens taktikutveckling*. Baserat på de historiska erfarenheterna av teknologisk utveckling är det troligt att denna debatt också kommer att driva på konceptuell och doktrinär utveckling av MDO. I detta sammanhang måste också hållas öppet för att mycket av doktrinutvecklingen inom MDO kan komma att stanna upp om USA väljer att helt vända ryggen till Europa.

Analysen ovan pekar således snarare mot en viss återhållsamhet vad gäller en återkommande kanonad av begrepp och förkortningar, och att det är på denna punkt som fokus på slagfältsnätverk respektive innovationsnätverk har en funktion. Oavsett vilken doktrinär förpackning, eller vilka modeflugor som kommer att prägla morgondagen, kommer chefer på strategisk, operativ och taktisk nivå att behöva ställa sig, tillfredsställande besvara och tydligt kommunicera två frågeställningar:

1. Hur förväntas mina underställda uppträda på slagfältet?
2. Hur ser mitt innovationsnätverk ut?

Det är ett faktum att både civil och militär teknik kommer att fortsätta utvecklas, men det viktiga för organisationsutvecklingen i Försvarsmakten är inte att vänta på att denna skall konceptualiseras och bli ännu en i raden av doktrinförkortningar. För oavsett förpackning behöver Försvarsmakten identifiera, upprätthålla och utveckla slagfältsnätverk och innovationsnätverk. Vägen framåt är således att inte förneka drivkrafterna för krigföringens utveckling, samtidigt med insikten att det inte finns ett enskilt koncept som utgör frälsningen för Försvarsmakten.

Författaren är lektor i krigsvetenskap vid Försvarshögskolan.

Noter

1. Denna artikel är en förkortad version av rapporten ”Nu är det väl revolution på gång?” (Försvarshögskolan, 2025). Författaren vill tacka Robert Dalsjö, Matthew Ford, David Gebre-Medhin, Aaron Jackson, John Nisser, Ove Pappila och Jan Ångström för kommentarer och synpunkter på rapporten.
2. NATO, *Alliance Concept for Multi-Domain Operations*, Enclosure 1, SHSDP/SDF/TT-010038, ACT/SPP/CNDV/TT-5856, 10 March 2023.
3. Pappila, Ove: ” Vad är Multi Domain Operations?”, *KKrVAHT*, nr 1/2025, s 54, 61.
4. Dekker, Ralph, Gubbels, Frank, Kalloniatis, Alex: “From Concept to Capability. In the NATO’s C2 of multidomain operations: history, evolution and challenges” Presented during the 29th International Command and Control research and technology symposium (ICCRTS), *NATO C2COE* 2024, s 10; Stubb, Alexander: *Tal för 254:e nationella försvarskursen*, 3 november 2025.
5. Detta har dock inte hindrat att intresset kring fenomenet växt: exempelvis har det har formats ett nätverk om MDO på Försvarshögskolan, och skolans Ove Pappila har känt sig manad att introducera fenomenet Pappila, 2025.
6. Allen, Patrick & Gilbert, Dennis: “Qualifying the Information Sphere as a Domain” *Journal of Information Warfare*, No. 3, 2010, s 42, författarens översättning.
7. FMV, Mot rätt insats… PE-studien – koncept och vision för adekvat insats (Stockholm: 2000).
8. Spirtas, Michael: ”Toward one understanding of multiple domains”, *RAND Commentary*, 2 May 2018.
9. Owens, Bill: *Lifting the fog of war* Farrar, Strauss and Giroux, 2000.
10. Se även Nisser, John: *Implementing Military Doctrine*, Doktorsavhandling, Försvarshögskolan, 2025.
11. Libiseller, Chiara & Michaels, Jeffrey H.: “Introduction to the special issue”, Special Issue: Fads and Fashions in Strategic Studies, *Journal of Strategic Studies*, No. 4, 2023.
12. Huntington, Samuel: “The lonely superpower”, *Foreign Affairs*, Vol. 78, No. 2, 1999.
13. Se exempelvis National Intelligence Council, (NIC), *Global Trends 2040. A more contested world*, 2021; Munich Security Conference (MSC) Report, *Lose-lose?*, 2024.
14. Dalsjö, Robert: ”Fångna av en stormvind”, *Axess*, mars 2024.
15. Tucker, Patrick: ”Biden Requests Less Than 1% Boost to Pentagon R&D, Despite Hyping New Defense Tech”, *Defense One*, 28 May 2021.
16. National Center for Science and engineering Statistics, (NCSES), *Analysis of Department of Defense Funding for R&D and RDT&E in FY 2022*. NSF 25-301, National Science Foundation, 2024.
17. Nouwens, Meia: “China’s dual use space sector goes global” *International Institute for Strategic Studies*, (IISS), July 2025; se även Funaiole, Matthew P. & Hart, Brian, “China’s Military in 10 Charts”, *Center for Strategic and International Studies* (CSIS) 2025.
18. Munich Security Conference (MSC) Report, *The Great Puzzle: Who will pick up the pieces?* 2019, s 52.
19. Gaida, Jamie, Wong-Leung, Jennifer, Robin, Stephan, Cave, Danielle: *ASPI’s Critical Technology Tracker. The Global Race for Future Power*, Australian Strategic Policy Institute (ASPI), Policy Brief 2023.
20. Det finns naturligtvis även andra påverkansfaktorer, som exempelvis en växande inrikespolitisk känslighet för militära förluster och svagare prioritering av militärutgifter.
21. Department of Defense, *Quadrennial Defense Review* Washington, 2014, s 22.
22. Tidigare försök av USA inkluderar den ”första kompensationsstrategin” som under 1950-talet ledde fram till de taktiska kärnvapnen, och den ”andra kompensationsstrategin” på 1970-talet som lade grunden till kryssningsmissiler, smygteknik och storskalig övervakningsteknik.
23. Christiansson, Magnus: “Defence planning beyond rationalism: the third offset strategy as a case of metagovernance”, *Defence studies*, No. 3, 2017.
24. Jag tackar Robert Dalsjö för denna poäng.
25. Hvizda, Mark, Frederick, Bryan, Laufer, Alisia, Evans, Alexandra T., Guiness, Kristen, Ochmanek, David A.: *Dispersed, disguised, degradable. The Implications of the Fighting in Ukraine for future U.S.-involved conflicts*, RAND Report 2024, s 13.

26. Watling, Jack, Zabrodski, Mykhailo, Danylyuk, Oleksander, Reynolds, Nick: "Preliminary Lessons in conventional Warfighting from Russia's Invasion of Ukraine", *RUSI*, February-July 2022.
27. Kayali, Laura: "France wants its own military AI algorithms", *Politico*, 7 February 2025.
28. Watling, Jack: *Emerging Approaches to Combined Arms Maneuver in Ukraine*, Insight Papers, RUSI, 2025; Watling et al.: "Preliminary Lessons in conventional Warfighting from Russia's Invasion of Ukraine", 2022; Garnier, Guillaume & Néron-Bancel, Pierre: *'At the other side of the hill': The benefits and false promises of battlefield transparency*, Ifri studies 2024.
29. Garnier & Néron-Bancel, *'At the other side of the hill': The benefits and false promises of battlefield transparency*, s 39.
30. Se exempelvis Hammes, Thomas X.: "Tactical Defense Becomes Dominant Again" *Joint Forces Quarterly*, 4th Quarter 2021, och Watling, Jack & Reynolds, Nick: "Stormbreak: Fighting Through Russian Defences in Ukraine's 2023 Offensive", Special Report, *RUSI*, 2023.
31. Pappila, 2025, " Vad är Multi Domain Operations?".
32. Skog Haslum, Ewa: "Introduction Regional Military Challenges", anförande på konferensen *Strategies, Deterrence and Resilience*, Kungliga Krigsvetenskapsakademien, 20 november 2025.
33. Försvarsmakten, *Doktrin Gemensamma operationer* Försvarsmakten, 2020, s 28.
34. Se även exempelvis Boot, Max: *War Made New. Technology, Warfare, and the Course of History 1500 to Today*, Gotham Books, 2006.
35. Citerad i Tucker, Patrick: "Move faster, share things: A former NATO transformation chief previews the summit" Defense One, 7 June 2025.
36. Gilli, Andrea, Gilli, Mauro, Grgic: "NATO, multi-domain operations and the future of the alliance", *Comparative Strategy*, Vol. 44, No. 1 2025, s 78; se även Trabucco, Lena & Salling Larsen, Esben: *Artificial Intelligence in Command and Control* Djøf Publishing, 2025.
37. Watling et al.: "Preliminary Lessons in conventional Warfighting from Russia's Invasion of Ukraine", 2022.
38. Hvizda et al.: *Dispersed, disguised, degradable. The Implications of the Fighting in Ukraine for future U.S.-involved conflicts*, s 2.
39. Se exempelvis Endsley, Mica R.: "From Here to Autonomy: Lessons Learned from Human-Automation Research", *Human Factors*, no. 59 2017, s 5–27; Endsley, Mica R.: "Theoretical underpinnings of situation awareness: a critical review" in Endsley, Mica R. & Garland, D. J. (eds.), *Situation Awareness Analysis and Measurement* Lawrence Erlbaum Associates, 2000.
40. Canovas, Juan: "Multi-Domain Operations and the Challenges to Air Power" *Joint Air Power Competence Center*, Joint Air & Space Conference 8-10 October 2019, s. 49.
41. Verney, Jean-Michel, Vicotte, Thomas, le Quement, Laurent, "Human-On-the-Loop": *Joint Air & Space Conference*, 7-9 September 2021, s 137.
42. NATO, *Command and Control (C2) Agility*, STO Technical Report, TR-SAS-085 2014, s 3.
43. Dekker et al: "From Concept to Capability. In the NATO's C2 of multidomain operations: history, evolution and challenges", s 10.
44. Försvarsmakten, *Arméns experiment med brigadledning vid MekB7* Delrapport 1 oktober Försvarsmakten, 2025, s 8.
45. Garnier & Néron-Bancel: *'At the other side of the hill': The benefits and false promises of battlefield transparency*, s 58; se även Marrow, Michael: "'Network-centric' security 'killing us' on JADC2 initiatives: USAF general", *Breaking Defense*, 11 July 2023.
46. Ellison, Davis & Sweijs, Tim: *Empty Promises? A year inside the world of multi-domain operations* Hague Center for Strategic Studies 2024.
47. Malow, Andreas & Blythe, Wilson C.: "Multi-Domain Warfighting in NATO. The 1 German-Netherlands Corps View", *Military Review*, May/June 2022, s 19.
48. Ellis, Patrick: "How the Army is putting the Commander Back in Command and Control", *War on the Rocks*, June 17 2025.
49. Freedman, Lawrence: "The Age of Forever Wars. Why Strategy No Longer Delivers Victory", *Foreign Affairs* May/June 2025.
50. Försvarsmakten, *Arméns experiment med brigadledning vid MekB7*, s 9.
51. Försvarsmakten, *Arméns experiment med brigadledning vid* MekB7, s 22.

52. I detta sammanhang är det viktigt att beakta att det finns behov av långräckviddig bekämpning på olika nivåer i alla tre försvarsgrenar. Jag tackar Ove Pappila för detta påpekande.
53. Watling, 2025, s. 22.
54. Försvarsmakten, *Arméns experiment med brigadledning vid* MekB7, s 14.
55. Försvarsmakten, *Arméns experiment med brigadledning vid MekB7*, s 16.
56. Försvarsmakten, *Arméns experiment med brigadledning vid MekB7*, s 21.
57. Se Magee, Aden: "The Sad and Sorry Tale of Cyber Command's Seven-Year Failure", *War on the Rocks*, September 4 2025 och Tollast, Robert: "The Time-Crunch for CyberEM Command's Challenges", *RUSI Commentary*, 15 July 2025 som varnande exempel.
58. Levinson, Daniel: "How to keep generative AI from crashing in combat", *War on the Rocks* 2025.
59. Jfr Plevnik, Mihael & Vuk, Pavel: "Navigating the uncertainty of the modern environment: multi-domain operations for the defence of small states", *European Security* 2025, s 1-28.
60. Howard, Michael: "Military Science in the Age of Peace", Chesney Memorial Gold Medal Lecture, October 3, 1973, printed in *RUSI* [Royal United Services Institute] *Journal* March 1974.
61. Utvecklingen går tydligen långsamt. Redan 2015 genomförde FOI en relevant förstudie (se Berglund, Erik, Hansson, Anders, Johansson, Peter, Johansson, Tommy, Larsson, Björn, Nygårds, Jonas: *Strid med system i samverkan. Teknisk förstudie* FOI, 2015).
62. Det finns även en mycket viktig etisk dimension, som berör närmast existentiella frågor som en konsekvens av den snabba utvecklingen av AI.
63. se exempelvis Dalsjö, Robert: "Det glesa slagfältet och försvaret av Sverige", *KKrVAHT*, nr 3/2019; Jensen, Benjamin & Macias, Jose M.: "Operational fires in the age of punishment", *Center for Strategic and International Studies* (CSIS) 2025.