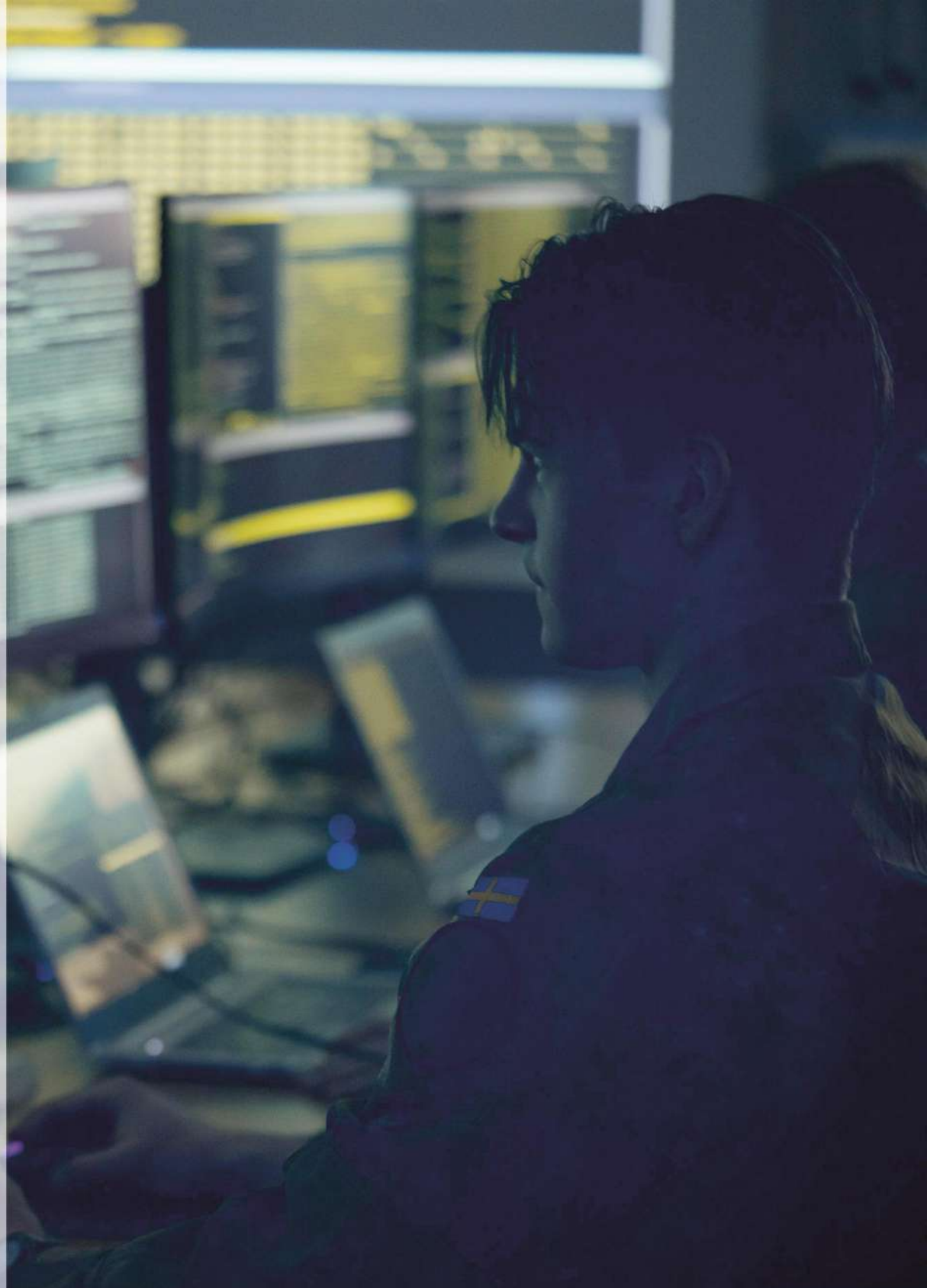


FÖRSVARSMAKTEN

2024



Rapport
**Fördjupade lärdomar och erfarenheter
från kriget i Ukraina**



Regeringskansliet
(Försvarsdepartementet) och
sändlista

Ert tjänsteställe, handläggare
Försvarsdepartementet

Ert datum
2023-07-13

Er beteckning
Fö2023/011323

Vårt tjänsteställe, handläggare
OPL J7

Vårt föregående datum
2023-11-02

Vår föregående beteckning
FM2023-2379:9

Fördjupade lärdomar och erfarenheter från kriget i Ukraina (3 bilagor)

Regeringen gav i juli 2023 Försvarsmakten i uppdrag att redovisa hur lärdomar och erfarenheter från kriget i Ukraina kan tillvaratas i Försvarsmaktens verksamhet och den fortsatta utvecklingen av det militära försvaret.¹ Den 2 november 2023 lämnade Försvarsmakten en delredovisning till regeringen.² En slutredovisning av uppdraget ska lämnas senast den 7 juni 2024. Denna rapport med bilagor är Försvarsmaktens slutredovisning av regeringsuppdraget.

Rapporten är ett komplement med fördjupningar till Försvarsmaktens delredovisning över lärdomar från kriget i Ukraina den 2 november 2023. Beskrivna erfarenheter och lärdomar omhändertas inom ramen för fortsatt utveckling av Försvarsmakten, exempelvis vid doktrinutveckling, planering, övning, träning och studieverksamhet. Dock betonar rapporten att Försvarsmakten behöver hitta nya former för hur erfarenheter och lärdomar implementeras. Det pågår därför utveckling av ett antal processer för att öka effekten av Försvarsmaktens erfarenhetshantering.

Försvarsmakten kommer att fortsätta analysera erfarenheter och lärdomar från kriget i Ukraina och utveckla formerna för detta. I samband med att myndighetens erfarenhetshantering utvecklas har detta samtidigt inneburit nya former och forum för samarbeten mellan försvarsmyndigheterna. Försvarsmakten kommer att fortsätta att sträva efter att gemensamt utveckla dessa samarbeten för att stärka förmågan att vara en lärande organisation.

¹ Regeringsbeslut, Fö2023/01323, 2023-07-13

² Försvarsmaktens lärdomar från kriget i Ukraina, FM2023-2379:9



Metod

Rapporten föreslår inte hur lärdomarna ska omhändertas, då det alltid finns en risk att observerade fenomen och erfarenheter från kriget är unika i tid och rum och därmed inte relevanta för framtidens krigföring. Rapporten betonar emellertid vikten av att omhänderta erfarenheter och lärdomar inkrementellt då det är troligt att beskrivna fenomen kommer att vara ingående komponenter i ett antal framtida konfliktscenarion.

Krigets dynamik innebär att en viss lärdom som är domänspecifik vid en tidpunkt förskjuts mot en annan domän vid en senare tidpunkt. Tempot i teknikutvecklingen och den taktikanpassning som sker under kriget innebär att det finns risker med att dra slutsatser utifrån enskilda erfarenheter. Kriget i Ukraina behöver analyseras utifrån en större kontext av andra krig och konflikter samt eventuella tekniksprång.

Rapportens syfte är inte att vara en heltäckande redogörelse av lärdomar och erfarenheter från det pågående kriget i Ukraina utan att presentera och analysera ett urval av observerade fenomen. Urvalet bygger främst på analyser och diskussioner som förts inom och mellan akademien och olika försvarsmakter som bedöms påverka utvecklingen av framtidens krigföring.

Försvarsmakten har kontinuerligt följt kriget i Ukraina och strävat efter att inhämta erfarenheter och information om kriget från en mängd olika källor. Dessa har omfattats av samarbetsländer, ukrainska företrädare, försvarsindustrin och relevanta myndigheter, särskilt i form av stöd från Totalförsvarets forskningsinstitut och Försvarshögskolan. Stödet har skett bland annat skett i form av seminarier, workshops, möten och intervjuer. Specialister inom olika områden har även bidragit med sakkunskap.

Läsanvisning

Kapitel 1 beskriver relevanta ukrainska erfarenheter med fördjupningar utifrån vad som beskrevs i Försvarsmaktens delredovisning till regeringen den 2 november 2023. Kapitel 2 beskriver och analyserar innebörden av dessa erfarenheter. Kapitel 3 beskriver och sammanfattar hur Sveriges och Natos krigföring skulle kunna utvecklas de närmaste åren.



Innehållsförteckning

Inledning.....	4
Putins krig?	4
Krigets dynamik	5
Rysk förmåga till militär anpassning.....	6
1. Det transparenta stridsfältet och den framtida operationsmiljön.....	7
1.1. Obemannade farkoster	8
1.2. Telekrig	9
1.3. Cyberdomänen	11
1.4. Rymddomänen	12
1.5. Stab- och ledningsplatsens överlevnadsförmåga	13
1.6. Skydd och verkan i informationsmiljön.....	14
1.7. Slutsats – vikten av överraskning, vilseledning och kamouflage	15
2. Tempot i krigföringen.....	17
2.1. Spridning och framskjuten ledning	17
2.2. Behovet av taktisk ISR-förmåga.....	18
2.3. Bekämpningskedjor – The Kill Web	19
2.4. Lägesbild och visualisering.....	20
2.5. Nyttjandet av civil kommunikationsteknik	21
2.6. Slutsats – fail fast, fail early!	22
3. Framtidens operationskonst.....	23
3.1. Behovet av enkelhet i en allt mer komplex värld	23
3.2. Operationskonst och decentraliserat beslutsfattande	23
3.3. Multidomänoperationer – en resa in i framtiden.....	24



Inledning

Putins krig?

*"[...] Crimea, the ancient Korsun or Chersonesus, and Sevastopol have invaluable civilisational and even sacred importance for Russia, like the Temple Mount in Jerusalem for the followers of Islam and Judaism."*³

Det finns anledning att betrakta det pågående kriget i Ukraina som en del i en mer omfattande stormaktskonkurrens. I den stormaktskonkurrensen utgår den ryska retoriken om kriget från ett antal antaganden om Rysslands historiska roll. Det ryska förhållningssättet om ett existentiellt krig i Ukraina är således betydligt mer långtgående än tidsperioden som rymmer president Vladimir Putins styre. Den västerländska föreställningen om kriget som "Putins krig" kan därför ses i ett större sammanhang.

Rysslands annektering av Krimhalvön 2014 kan i den historiska kontexten ses som ett militärstrategiskt val för att behålla Rysslands tillgång till en isfri hamn i Svarta havet, vilket Ryssland har eftersträvat sedan Katarina den storas tid och Svartahavsflottans skapelse. Kristnandet av Kievriket under 900-talet skildrar begynnelsen av den ryska skapelsemyten, det vill säga berättelsen om hur Ryssland och dess världsuppfattning bildades. Det var detta resonemanget som Putin valde att framföra till den ryska befolkningen i sitt tal till nationen 2014 för att förklara och rättfärdiga annekteringen av Krim. Med Putins egna ord var det heller inte möjligt att tillåta "Nato-stövlar" på mark som är helig för Ryssland.

Sevastopol på Krimhalvön har varit den ryska Svartahavsflottans bas i över 200 år och är en av tolv sovjetiska hjältestäder. Sevastopol är därför central för den ryska krigsmaktens mytbildning. Ryssland har under ett antal krig tidvis förlorat staden vilket har lett till nationella sår. Ryssland och Ukraina har vid flera tillfällen efter Sovjetunionens upplösning förhandlat om att även fortsättningsvis tillåta Ryssland att nyttja stadens flottbas.

Kriget i Ukraina ingår i ett ryskt resonemang om ett existentiellt krig som förknippas med skapelsemyten i form av narrativet om ett fosterländskt försvarskrig där väst agerar som angripare. Idag använder Putin idén om ett fosterländskt krig i syfte att stärka den nationella sammanhållningen och motivera Rysslands krigsföring. Oavsett antaganden om huruvida kriget kommer att fortsätta efter Putin kommer den ryska krigsmakten att fortsätta att utvecklas och anpassas, både doktrinärt och förmågemässigt.

³ Putin, Vladimir. 2014. *Presidential Address to the Federal Assembly*.
<http://en.kremlin.ru/events/president/news/47173>



Krigets dynamik

Kriget består av två postsovjetiska militära system som möter varandra vilket präglar krigföringen. Båda sidor använder ny materiel och teknik samt utvecklar taktik och stridsteknik, huvudsakligen för att överleva på slagfältet och begränsa motståndarens handlingsförmåga. Ukraina har fått stöd och råd från flera västerländska länder. Det innebär att Ukraina utvecklar en hybrid av sovjetiskt tänkande, västerländska influenser och nytt tänkande med hänsyn till egna erfarenheter. Däremot har inga nya operativa koncept eller principer ännu observerats.

Nästan inga gemensamma operationer har genomförts och har ibland helt eller delvis övergivits till förmån för ensidiga ambitioner inom en specifik domän. Det har visat på vikten av att skapa dilemman för motståndaren i alla domäner och på alla nivåer av krigföring för att tvinga denne att prioritera och därigenom behålla initiativet. Kriget har även lett till utnötning av och slitage på både Rysslands och Ukrainas traditionella militära plattformar. Stridsvagnar och pansarfordon förstörs ofta av svårupptäckta obemannade plattformar som är små, snabba, billiga och lätta att utveckla, istället för i stora strider. Ukraina har också sänkt en tredjedel av den ryska Svartahavsflottan, inte genom stora sjöstrider, utan genom att använda obemannade farkoster.

Den inledande ryska invasionen 2022 var ett misslyckande, och den efterföljande perioden med striderna i Donbas kännetecknades till en början av ryskt dominerande eldöverlägsenhet. Förutom precisionsammunition förbättrades även användningen av obemannade farkoster för måldetektering effektiviteten i de äldre ryska artillerisystemen. Ryska artilleribatterier som använde obemannade farkoster för måldetektering visade sig även kunna beskjuta ukrainska positioner inom ett par minuter efter att de upptäckts. Detta tvingade ukrainska infanterikompanier till ökad spridning för överlevnad. Följaktligen täckte bataljoner frontbredder som traditionellt är en brigads ansvar. Rysk artilleriöverlägsenhet och sensortäthet förhindrade även ukrainarna från att koncentrera sig i enheter över kompanistorlek, eftersom större förbandsformationer skulle upptäckts i förtid och kunna bekämpas effektivt på stora avstånd.

Både Ryssland och Ukraina har haft integrerade luftförsvarssystem som är tillräckliga för att framgångsrikt förneka den andra parten att skapa tillräcklig kontroll över luften. Det innebär att ingen av sidorna har haft tillräcklig förmåga att uppnå luftherravälde. Ukraina har emellertid behållit en central ledning av sina luftstridskrafter. Detta har fått positiv inverkan på förmågan att över tid nå verkan med sina förband mot en kvalificerad motståndare. Inte minst har Ukraina uppvisat förmåga att upptäcka och bekämpa ryska fjärrstridsmedel som kryssningsrobotar och ballistiska robotar.



Lärdomen är att stridsfältsförhållandena kan försvåra möjligheten att kraftsamla för att genomföra offensiva operationer. Detta minskar sannolikheten för storskaliga strider och nödvändiggör därmed en synkronisering av effekter, snarare än en traditionell koncentration av förband. Detta lägger i sin tur en extra börda på ledningsförmågan, särskilt när den försvåras av elektronisk krigföring. Dessutom strävar både Ryssland och Ukraina efter överlägsenhet i sina respektive bekämpningskedjor samtidigt som de prioriterar att störa varandras bekämpningskedjor.

Rysk förmåga till militär anpassning

Det pågående kriget i Ukraina har agerat katalysator för taktisk och militärteknologisk anpassning. Både Ryssland och Ukraina har behövt ställa om och anpassa sina samhällen utifrån krigets krav. Båda länderna genomför anpassningar genom att lära sig av och sprida de erfarenheter som de fått i kriget.

Den ryska krigsmakten präglas av toppstyrning, ett arv från sovjettiden som inledningsvis försvårade militär anpassning. Samma toppstyrning används nu av den militära ledningen för att undanröja hinder för anpassning och systematisera förändringen genomgående i den ryska försvarssektorn. Det som fortfarande hämmar rysk anpassningsförmåga är rädslan för repressalier vid rapportering av misslyckanden inom den ryska krigsmakten.

Två andra faktorer som lett till att den ryska anpassningsförmågan har förbättrats sedan krigsutbrottet är omställningen till krigsekonomi och samarbete med länder som Kina, Iran och Nordkorea. Detta har möjliggjort ökad produktion av krigsmateriel, bland annat ammunition och drönare. Den ökade produktionen har i sin tur resulterat i större handlingsfrihet att införa militära anpassningar. Sammanfattningsvis uppfattas Ryssland som en förändringsbenägen motståndare vars verktygslåda har få begränsningar när syftet är att fullfölja sina långsiktiga strategiska mål, men där taktiken fortfarande till stor del bygger på ett utnötningskrig och där den ryska inställningen och innovationsprocessen på högre nivå har präglats av "mer av allt".



1. Det transparenta stridsfältet och den framtida operationsmiljön

"You go to war with the army you have, not the army you might want or wish to have at a later time."⁴

Detta kapitel beskriver ett antal observationer från kriget i Ukraina som visar på utveckling av krigföringen. Det mest framträdande fenomenet är att kriget, efter den ukrainska offensiven våren 2023, har utvecklats till ett ställningskrig där både Ryssland och Ukraina haft svårt att bryta igenom varandras försvarslinjer, bland annat på grund av omfattande fältarbeten som skyddas av mineringar och artilleri. Dessutom skyddas försvarslinjerna av en sensortät stridsmiljö som döpts till det transparenta stridsfältet.

Försvarslinjerna, framför allt de ryska, består av en kombination av omfattande fältarbeten såsom skyttegravar, taggtråd och stridsvagnshinder som skyddas av mineringar och artilleri. Den ryska förmågan att återminera minbrutna anfallsstråk med avståndslagda minor är en utmaning för ukrainska motanfall. Detta har lett till att ryska förband kunnat behålla kontrollen över stora landområden där det inte funnits några framryckningsbara luckor i mineringarna.

Det transparenta stridsfältet innebär att operationsmiljön är översvämmat av olika typer av sensorer, men främst av obemannade farkoster, och att all trupprörelse och militär verksamhet är minutiöst övervakad, särskilt inom markdomänen. Det transparenta stridsfältet är inte lika uppenbart inom sjödomänen, men dess närvaro får många gånger mer långtgående och emellanåt till och med globala följder. Det transparenta stridsfältet har i Ukraina fått konsekvensen att det säkraste sättet att överleva är spridning till den grad att det har försvårat kraftsamling. Kriget utkämpas nu huvudsakligen av mindre enheter som varit svåra att samordna för att uppnå operativ effekt, både offensivt och avseende att hålla tagen terräng.

Eftersom det transparenta stridsfältet även för med sig ökad precision för långräckviddig bekämpning har båda sidor dragit tillbaka lednings- och logistikresurser så långt som möjligt från fronten. Båda sidor fortsätter att anpassa sig, men hittills har ingen sida uppnått några nya operativa eller militärstrategiska avgöranden på grund av att förmågan till kraftsamling saknas. Markkriget behöver också ses utifrån avsaknaden av luftherravälde och att det råder en obalans inom och mellan de olika domänerna.

Det transparenta stridsfältet, framförallt via obemannade farkoster, har stegrat tempot i katt-och-råtta-leken mellan att vara den som bäst kan gömma sig och vara den som är bäst på att slå till först. Den stora mängden sensorer kombinerat

⁴ Rumsfeld, Donald. 2004. *Troops Question Secretary of Defense Donald Rumsfeld about Armor*. <https://www.pbs.org/newshour/show/troops-question-secretary-of-defense-donald-rumsfeld-about-armor>



med taktikanpassningar som baserats på erfarenhetshantering har lett till att båda sidor ständigt förbättrat tempot i sina bekämpningskedjor. I tidigare krig och konflikter har västländers drönare för spaning, lokalisering, målföljning och utvärdering varit en exklusiv och kostsam resurs. Kriget i Ukraina visar att relativt billiga drönare kan användas för dessa ändamål i nästan alla domäner, inklusive att störa globala navigeringssystem (GNSS).

1.1. Obemannade farkoster

Obemannade farkoster, så kallade drönare, är det område som uppvisat störst bredd av både behov och lösningar, och som präglas av ständiga förändringar och anpassningar. Det nya är att drönare nu alltmer används inom sjö- och markdomänen. Drönanvändningen har utvecklats även i luftdomänen med fler användningar, nya motmedel och drönartyper, framförallt *first-person view*-drönare.⁵ För att täcka upp för de enorma förlusterna av farkoster, i vissa fall uppskattat till 10 000 stycken per månad, anskaffas stora mängder kommersiella system som anpassas i Ukraina och nära stridsfältet. Utvecklingen av obemannade farkoster visar att de både använts som förmågeförstärkare och mot en helt egen funktion eller stridskraft. I februari 2024 upprättade Ukraina exempelvis en ny försvarsgren för obemannade system.

Under kriget i Ukraina har framför allt nyttjandet av obemannade farkoster medfört att det är näst intill omöjligt att dölja sig på stridsfältet. Detta gäller främst markdomänen, men där utvecklingen inom sjödomänen framträder allt mer innovativt. Till detta ska tilläggas att nästan all fysiskt synlig infrastruktur är kartlagd av olika sensorer. Obemannade farkoster har den fördelen att en och samma plattform kan användas till både spaning, övervakning och bekämpning till en relativt låg kostnad. Den låga kostnaden innebär även att stridsfältet kan översvämmas med drönare för att mätta ett eventuellt försvar. Självmoordsdrönare, så kallade kamikazedrönare, har beskrivits som den mest effektiva typen av obemannade vapensystem och ett större hot än konventionellt artilleri, med tillägg för ett eventuellt ändrat uppträdande på grund av brist på kraftsamling av artilleri.

Drönare används också i allt större utsträckning som skenmål för att förmå försvararen att aktivera sina luftförsvarssensorer, som då kan målbestämmas och bekämpas. Även detta tillvägagångssätt är ett exempel på att precisionsbekämpning genom en fungerande bekämpningskedja som ständigt anpassas efter nya förhållanden, är effektivare än yttäckande artilleribekämpning, något som båda sidor har lärt sig att skydda sig mot.

⁵ En drönare med en kamera som direktöverför vad den ser till operatören, oftast via ett par glasögon.



Utmaningen med fjärrmanövrerade och autonoma system är att många system är beroende av det elektromagnetiska spektrumet som därmed kan påverkas med telekrigssystem.⁶ Fjärrmanövrerade och autonoma system i sjödomänen är redan idag i högre grad oberoende av GNSS och inte lika bundna till det elektromagnetiska spektrumet som luftburna system. Hit räknas bland annat torpeder, minor och olika fjärrstyrda obemannade farkoster.

Utvecklingen inom luftdomänen går mot att försöka göra systemen mindre sårbara för störningar genom att göra dem mer autonoma och minska beroendet av lägesinformation från globala navigeringssystem. Kommunikationslänkarna modifieras också för att använda andra frekvenser i försök att undgå störning, vilket i sin tur kräver snabb anpassning av motmedelssystemen. Vidare uppträder systemen numera ofta i förband med större farkoster i tillbakadragna roller som sambandsrelä med mindre system som är mer svårupptäckta över fientligt kontrollerat territorium.

Lärdomen för Försvarsmakten är att öka tillgången till olika typer av obemannade farkoster för att lära sig använda dessa effektivt, och hur man bäst försvarar sig mot drönare under olika förhållanden. Det behöver skapas förutsättningar för att kunna öva med och mot drönare på alla nivåer. Detta behöver göras brett inom Försvarsmakten eftersom olika typförband har olika behov och förutsättningar. De många olika typer av skyddsobjekt har också olika förutsättningar för hur de bäst kan skyddas.

Utmaningen med att utveckla effektiva motmedelssystem mot drönare (C-UAS) är den stora variationen av drönare som skyddet ska kunna hantera. Det gäller att kunna skapa flera lager av skydd, exempelvis genom rörelse, hastighet, störförmåga, kamouflage, skenmål, närluftvärn och nät, eftersom det för tillfället inte finns ett enskilt heltäckande system. Denna problematik har lett till en återupptäckt av betydelsen av fysiskt skydd och ingenjörförband för såväl den taktiska nivån som för operativ logistik och ledning. För att tydliggöra alla dessa behov och begränsningar bör detta område fortsätta att studeras med stöd av andra myndigheter, men samordnat av Försvarsmakten utifrån en gemensam målbild för totalförsvaret.

1.2. Telekrig

Kriget i Ukraina har aktualiserat behovet av att kunna verka och förstå sin egen signatur i det elektromagnetiska spektrumet, allt från positionssystem, gemensam och säker tid för kommunikation och inte minst för att styra fjärrmanövrerade farkoster eller använda autonoma system. Omfattande telekrigsinsatser, såväl störning som spaning, visar på vikten av att behärska sin signatur i eteren och att kunna välja och veta när det inte är lämpligt att sända. Ett felaktigt beslut leder till bekämpning, ofta inom kort tid. Både Ryssland och Ukraina har under kriget

⁶Inom 12 månader från det att självmordsdrönare började användas på bred front med styrlänkar på 900 MHz-bandet hade Ryssland fått ut motåtgärder i fält.



använt hela det elektromagnetiska spektrumet för att kommunicera och några civilt fredade frekvensområden finns knappast kvar. Istället har möjligheten till transmission mångfaldigats genom att använda både kommersiella och militära kommunikationssystem.

Kampen mellan medel och motmedel stimulerar en teknikutveckling inom telekrig som sker i så högt tempo att ny teknik snabbt kan bli föråldrad. Ett vanligt exempel är att störa satellitsystem från drönare eller markburna störsändare. Dessa störsystem varierar från stora markburna högeffektssystem till mikrosystem med låg effekt, men som räcker exempelvis till att hindra rymdbaserade sensorer från att identifiera fordonstyper. Konsekvensen av detta är ett behov av en telekrigsförmåga med hög grad av automatisering som snabbt anpassar sig till förändringar hos motståndarens tekniska system. Denna teknik har varit relativt dyr och exklusiv, men den trånga sektorn idag utgörs mer av kompetenser inom området. Att störa med tunga system på bred frekvens och med hög effekt medför riskerna att störa ut egna system och röja störsystemens position. Det mest lockande alternativet är att använda många mindre, lätta och rörliga system, vilket dock kan kräva att man gör avkall på automatisering, då mindre och lätta system oftast saknar denna kapacitet. Oavsett lösningar behöver en effektiv telekrigsförmåga kombineras med frekvensplanering och samordning.

Trots telekrigsförmåga och signalspaning fortsätter båda sidor i kriget att nyttja mobiltelefonnätet och internet, om än på olika sätt. Användandet av mobiltelefoner och militära radiosystem vid frontavsnitt har fortsatt inneburit en hög risk för bekämpning. Bekämpning kan ske inom minuter från att ett mobilsamtal påbörjats. Därför används applikationer som *Discord*, *Telegram*, *Signal* och *WhatsApp* i högre grad än mobilsamtal och militära radiosystem, eftersom en kombination av olika internetlösningar upplevs som säkrast och där det kommersiella satellitsystemet *Starlink* används frekvent. Det som ukrainare betonar är dock vikten av att få ut information snabbt och på stor bredd. Dessa applikationer erbjuder även en ökad möjlighet till överföring av bild- och videobaserad information, som bland annat underlättar delning av data inhämtad av drönaroperatörer.

Att använda kommersiella applikationer eller bredbandsinfrastruktur innebär risker, exempelvis för avlyssning. För Ukraina har fördelarna hittills övervägt nackdelarna och den eventuella ryska förmågan till signalspaning, eller inhämtning inom cyberdomänen har inte haft någon betydande effekt. Oavsett är detta ett exempel på hur olika domäner och funktioner interagerar med och i varandra, vilket visar att Försvarsmakten behöver ha förmåga att spana mot och påverka såväl militära som kommersiella system samtidigt. Ett delegerat mandat för telestörinsatser har visat sig vara avgörande i såväl offensiva som defensiva operationer.



1.3. Cyberdomänen

Cyberattacker har varit ett återkommande inslag och riktats mot olika sektorer av ett alltmer digitaliserat Ukraina. Sedan krigets start 2014 har det ukrainska samhället behövt skapa en organisationsstruktur, centralt och lokalt, som kan hantera cyberhot och hålla militära och kommersiella ledningsstödsystem i drift. Att samordna samhällets cybersäkerhetsresurser, inklusive volontärer, har varit en central erfarenhet där kraven på informationssekretess, och informationens riktighet och tillgänglighet har vägts av med ett operativt perspektiv. Erfarenheterna från kriget i Ukraina visar på vikten av att ha kompetens inom cyberområdet och incidenthanteringsförmåga såväl i lokala driftorganisationer som centralt för att skapa en robust organisation.

Nästan alla analoga sambandssystem fasas ut allt eftersom system kopplas mot nätverk. Därför blir det allt viktigare att ha ett cyberförsvar på plats. Detta gäller även militära system då exempelvis rymdbaserade resurser, telekrigsresurser och andra sensorer kombinerat med artificiell intelligens behöver integreras via ledningsstödsystem för att få operativ effekt. Sammantaget tenderar digitaliseringen av samhället där fysiska system integreras i hög grad att leda till att telekrig, signalspaning, ledningssystem och underrättelseinhämtning får betydelse även i förhållande till cyberdomänen.

Ukraina har visat hur cyberdomänen rent praktiskt kan integreras i gemensamma operationer genom att använda cyberresurser för att hitta lämpliga mål. Detta kan ske antingen reaktivt genom att exploatera IT-sårbarheter hos ett redan identifierat högvärdigt mål eller proaktivt genom att aktivt söka efter sensorer som motståndaren har uppkopplade via internet (exempelvis fjärrstyrda kameror). Därtill har utvecklingen inom artificiell intelligens öppnat upp för nya möjligheter inom cyberdomänen, särskilt i underrättelsesyfte för analys av bild och film, till och med på taktisk nivå exempelvis för att nästan i realtid kunna följa trupprörelser.

Den kontinuerligt ökade mängden programvara i militära system innebär ett ökat behov av att kontinuerligt skydda system, data och information samt att programvaror uppdateras samtidigt som informationen behöver göras tillgänglig. Erfarenheterna från kriget i Ukraina visar även på att digitaliseringen av samhället innebär ett behov av en sammanhållen cyberförsvarsförmåga med likriktade strukturer på alla ledningsnivåer som även behöver inkludera förmågan till inhämtning inom cyberdomänen som kan bidra till en gemensam bekämpningsfunktion.



1.4. Rymddomänen

Idag sker ett antal samtidiga omvälvningar av rymddomänen på global nivå. Dels genomgår länder ett paradigmskifte till att betrakta rymden som en militär operationsdomän och anpassar militära strukturer och förmågor därefter, dels spelar kommersiella rymdsystem en allt viktigare roll i modern krigföring. Det senare har synliggjort otydligheten kring huruvida kommersiella rymdsystem ska ses som civila eller militära objekt vid militära angrepp, en fråga där det inte etablerats internationell konsensus. För Ukraina har användandet av kommersiella rymdsystem inneburit en ökad säkerhet då dessa inte otvetydigt kunnat klassas som militära mål av Ryssland, även om Ryssland under kriget allt mer uttalat att även kommersiella satelliter som bidrar till kriget kan komma att klassas som legitima militära mål.

Ryssland är idag försvagat i sin ställning som den tredje rymdstormakten, och är tydligt efter USA och Kina vad gäller såväl teknologi som numerär. Trots det ska den ryska förmågan att nyttja rymdsystem för militära ändamål inte underskattas. Även om Ryssland står inför stora och mångfacetterade utmaningar inom rymddomänen så har landet en stor bredd av rymdbaserade förmågor och rymdförnekande förmågor som syftar till att nedsätta andra aktörers användande av sina rymdsystem.

I kriget i Ukraina har rymdbaserade system använts som förmågeförstärkare av både Ryssland och Ukraina. Exempelvis har kombinationen av rymdsystem med obemannade farkoster och långräckviddiga bekämpningsmedel visat sig skapa förmåga att slå på djupet. Tanken är förvisso inte ny, men då tekniken inom dessa system blir allt mer tillgänglig innebär det att dessa resurser kan användas på samtliga ledningsnivåer och därmed ge en förändrad förmåga att både slå på djupet och att skydda taktiska resurser.

Kommersiella rymdsystem har i Ukraina använts i krigföringen i en aldrig tidigare skådad utsträckning. De kommersiella systemen består ofta av större konstellationer på uppemot flera hundra satelliter, som enskilt kan vara lägre presterande men där mängden möjliggör helt andra tjänster än militära system, som traditionellt bygger på större enstaka satelliter med hög prestanda. Detta, i kombination med rymddomänens ständiga utveckling, inklusive offensiva rymdförmågor ställer frågor som huruvida det är lämpligt att införskaffa få och dyra satelliter då det kan skapa en stor sårbarhet i systemet. Billigare och därmed fler satelliter skapar redundans och säkrare tillgång till rymdtjänster, även om en eller flera satelliter störs ut eller påverkas på annat sätt. Det gör det också möjligt att i högre grad separera civil och militär användning av satelliter.

Kommersiella jordobservationssatelliter gjorde att allmänheten redan före invasionens början kunde följa rysk truppuppbyggnad i media genom dagsfärskas bilder. Dessutom kunde underrättelser och analyser lättare delas mellan olika länder då dessa utåt kunde underbyggas med offentliga bilder utan att röja egen militär inhämtningsförmåga. Ukraina har upphandlat stora mängder kommersiell



jordobservationsdata, men även genom så kallad *crowdfunding* köpt en ICEYE SAR-radarsatellit. Uppgifter gör gällande att denna satellit bara under de första två dygnen upptäckte 60 ryska enheter, vilket ledde till att Ryssland förlorade materiel till ett värde långt större än den totala kostnaden för satelliten. Detta visar tydligt på vilken nytta satelliter kan ha som förmågeförstärkare för andra militära system.

Kriget i Ukraina har visat att satellitsystem kan ha en stor betydelse både för militären och civilsamhället. Detta har lyft fokus mot vikten av att rymdinfrastruktur med dess förmågor består under en konflikt och inte störs ut eller bekämpas. *Starlink* som försett Ukraina med kommunikation och internet har under kriget aktivt behövt uppdatera sin cybersäkerhet för att möta angrepp som syftar till att påverka systemet. Det är även uppenbart att en styrka i *Starlink* ligger i mängden satelliter systemet består av, samt hastigheten och förmågan hos *SpaceX* att kunna sända upp nya satelliter. Lärdomen för totalförsvaret är att för länder som vill ha egna satellitsystem för olika ändamål så är det uppenbart att säkerheten, skyddet och försvaret av de egna rymdförmågorna är av största vikt.

1.5. Stab- och ledningsplatsens överlevnadsförmåga

Det transparenta stridsfältet i kombination med fler och billigare vapensystem med allt längre räckvidder skapar betydande hot mot ledningsplatser, såväl fasta som rörliga. Detta ska läggas till en utveckling varigenom staber har vuxit och ledningsplatser kommit att innefatta större mängd teknik. Större ledningsplatser skapar mer rörelse samt avger dessutom en större elektromagnetisk signatur och emittering, vilket gör det lättare för en motståndare att upptäcka ledningsplatser via drönare, signalspaning, inhämtning i cyberdomänen och satellitsystem.

Att ledningsplatser, framförallt i västländer, har ökat i storlek är en följd av ökningen i stridsfältets komplexitet, dels i form av hybrida hot, dels i form av att teknikutveckling lett till att domänerna påverkar och integrerar i varandra i allt högre grad. Debatten om att öka ledningsplatsers överlevnadsförmåga har kretsat kring traditionella frågor om självskydd såsom maskering, skenåtgärder samt fysiskt skydd inklusive luftvärn och *C-UAS*.

Svårare frågor inom området ledningsförmåga är hur ledningsplatser kan minskas i omfång, hur ledningsresurser kan spridas mer, hur kamouflage kan förbättras och hur det logistiska och elektromagnetiska fotavtrycket kan minskas.

Maskering är betydligt enklare och billigare avseende optiskt kamouflage, medan akustiskt, termiskt och elektromagnetiskt kamouflage är betydligt mer kostsamt. Att minska det logistiska fotavtrycket är möjligt genom att exempelvis ha strikta rutiner för flöden till och från ledningsplatser och där vissa varor och tjänster kan levereras via obemannade farkoster.



Den stora utmaningen ligger i att minska det elektromagnetiska fotavtrycket, särskilt då spridning leder till en ökad transmission och därmed emittering. Inom detta område har ett antal lösningar framkommit i den militära debatten. En lösning är att, i den mån det är möjligt enligt folkrätten, gruppera ledningsplatser bland befintlig infrastruktur där emittering inte sticker ut i någon högre grad. En annan lösning är att i högre grad nyttja kommersiella kommunikationssystem för att på så sätt dölja militär signaltrafik. Ett annat exempel är att nyttja sambandsteknik med en smal och riktad emittering, exempelvis laser. Med all sannolikhet är ingen enskild lösning tillräcklig; istället kommer en kombination av åtgärder krävas för att i möjligaste mån dölja egna ledningsresurser.

1.6. Skydd och verkan i informationsmiljön

Ukraina har sedan den storskaliga invasionen 2022 haft två huvudsakliga kommunikationsstrategiska målsättningar. För det första att upprätthålla befolkningens försvarsvilja och för det andra att säkra västvärldens stöd. Ett fåtal övergripande narrativ har nyttjats för att anpassa kommunikationens anslag och form för att nå olika målgrupper. För att säkra västvärldens fortsatta stöd i kriget har Ukraina bland annat lanserat kampanjer i sociala medier som riktar sig till befolkningarna i de länder som har donerat vapensystem. I kampanjerna tackar Ukraina ländernas befolkningar, ofta med ett humoristiskt anslag.

Ukraina har skapat en bred situationsförståelse och lägesbild i relation till Ryssland. Kreativitet och strävan efter ett informationsöverläge har bidragit till framgångar i informationsmiljön i samverkan med underrättelsetjänsten och internationella aktörer. Ytterligare framgångsfaktorer som den ukrainska försvarsmakten angett är att samordna tillgängliga resurser och att samarbeta med externa aktörer. Detta har varit en förutsättning för att kunna hålla ett högt tempo, tillföra nya idéer efter hand och publicera kommunikation på flera olika språk.

Media har en viktig roll i hur bilden av kriget förmedlas och därmed uppfattas av olika aktörer. I samband med krigsutbrottet utlystes krigslagar och kort därefter kom en order från överbefälhavaren om militär censur. Detta har inneburit stor påverkan på medias förutsättningar att rapportera om kriget. Vid ett utdraget krig kan det bli en utmaning att balansera statens intressen med journalistisk integritet och medias oberoende. Ukraina har i detta avseende andra förutsättningar än Sverige, men frågan om rollen för public service i händelse av krig är komplex, bland annat då det finns en utmaning i att hitta en balans mellan behovet av operationssekretess och transparens i kommunikationen.

För att göra avtryck i informationsmiljön och vinna kampen om narrativet är det av vikt att hela organisationen strävar mot samma kommunikationsstrategiska målsättningar och effektmål. Dessa mål och effekter bör vara tydliga men övergripande. Uppdragstaktik ses som nödvändigt för att kunna agera snabbt i informationsmiljön och för att vinna kampen om narrativet. Därtill finns det ett behov av en robust och väl spridd förmåga till stridsfältsdokumentation i händelse



av krig eftersom det är en framgångsfaktor att snabbt kunna använda relevant bildmaterial i kommunikationen.

Samhällets förmåga till kommunikation och informationsöverlägsenhet bygger på att det finns en motståndskraftig informations- och kommunikationsinfrastruktur. I början av den fullskaliga invasionen angrep Ryssland Ukrainas markbundna kommunikationsinfrastruktur samtidigt som satellitföretaget *Viasat* utsattes för ett cyberangrepp. Lösningen på detta var att *Starlink* på bred front introducerades i Ukraina. *Starlink* har även medfört att information kunnat flöda både in och ut ur Ukraina, något som även hjälpt civilbefolkningen att hålla sig uppdaterade kring händelseutvecklingen, men även för att kunna sprida information om hur livet i krigets Ukraina ser ut och vilket behov av internationellt stöd som finns.

Situationsförståelse, informationsöverläge, narrativägende och därefter förmåga att orkestrera och manövrera, det vill säga kontinuerligt anpassa kommunikationen för att uppnå önskade militärstrategiska effekter, är en process som ständigt behöver pågå. Lärdomen för Försvarsmakten och totalförsvaret är att resurser för att planera, genomföra och analysera effekter och kommunikativt utfall för egen del och för motståndaren behöver vara igång tidigt och att det är en förutsättningsskapande resurs för gemensamma operationer.

1.7. Slutsats – vikten av överraskning, vilseledning och kamouflage

Det transparenta stridsfältet har förnyat synen på överraskning, vilseledning, maskering, kamouflage och skenmål. Detta gäller all militär verksamhet och i alla domäner. Därtill har även civila resurser som exempelvis ambulanser och räddningsfordon tvingats att kamoufleras för att undgå bekämpning. Konsekvensen av det transparenta stridsfältet, i kombination med avsaknaden av luftherravälde, har bidragit till en oförmåga att kraftsamla i rum. Förmågan att kraftsamla, leda större förband och genomföra gemensamma operationer var dessutom begränsad innan kriget utvecklades till ett ställningskrig.

Det transparenta stridsfältet har även visat på svårigheten att genomföra överraskning och vilseledning på stridsteknisk och taktisk nivå. Lärdomen är att det senare behöver planeras och samordnas på militärstrategisk och operativ ledningsnivå för att nå operativ effekt. Krig avgörs ytterst genom politiska handlingar, men oftast följer detta på operativa avgöranden. Operativa framgångar möjliggörs i sin tur av anpassningsförmåga med innovativa lösningar, både på taktisk, operativ och militärstrategisk nivå. Erfarenheterna från Ukraina visar exempelvis på att falsksignalering och informationsoperationer sker på samtliga ledningsnivåer.

Försvarsmakten behöver en väl utvecklad förmåga att dölja sig i det transparenta stridsfältet och samtidigt ha förmågan att mätta motståndarens system. Det kräver att Försvarsmakten testar, övar, prövar och utmanar organisationen. Det inkluderar nyttjandet av överraskning, vilseledning, maskering, kamouflage och



skenmål samt åtgärder för att minska emittering. Detta kräver att Försvarmakten övar och nyttjar så kallade *Red Teams*⁷ med mandat och resurser att spana akustiskt, optiskt, termiskt och elektromagnetiskt för att bygga en förståelse för hur Försvarmakten ser ut i motståndarens ögon. Av denna anledning behöver lagstiftning och regelverk ha beredskap att uppdateras i takt med utvecklingen och då särskilt hur den lägre delen av luftrummet ska regleras och samordnas. Regelverk behöver beakta behovet av att samordningen och regleringen kan genomföras i högt tempo, både avseende underrättelseinhämtning, spaning, ytövervakning, skydd och bekämpning.

⁷ Red Team-testning nyttjas antingen för att utvärdera den egna organisationen genom att simulera en hotaktörs angreppsmetoder eller för att generera alternativa handlingsalternativ.



2. Tempot i krigföringen

”Operational tempo is a state of mind.”⁸

Det pågår en debatt inom både akademien och den militära professionen om hur utvecklingen av krigföringen i Ukraina kommer att påverka militär verksamhet, teori och doktrin – nu och i framtiden. Detta mot bakgrund av att kriget i Ukraina har lett till ett ökat fokus på behovet av flexibilitet och militär anpassningsförmåga framförallt då teknikutvecklingen har öppnat upp för nya möjligheter och samtidigt skapat nya utmaningar. Detta kapitel beskriver dessa möjligheter och utmaningar.

Enligt taktikens grunder behöver det skapas tillräckligt gynnsamma förutsättningar i relation till den aktuella motståndaren, något som brukar kallas lokal överlägsenhet. Den lokala överlägsenheten kan skapas genom kraftsamling, överraskning och handlingsfrihet. Det transparenta stridsfältet har i Ukraina kraftigt försvårat möjligheten till både överraskning och kraftsamling, vilket i sin tur har lett till begränsad handlingsfrihet i att uppnå verkan. För att lyckas med kraftsamling måste detta ske i ett så pass dolt eller högt tempo att motståndaren inte lyckas vidta några motåtgärder. Ett högt operativt tempo kräver i sin tur förmåga att leda och samordna striden samt god tillgång till underrättelser.

Teknikutvecklingen och det transparenta stridsfältet visar på vikten av att ha snabbare beslutscykler än motståndaren. Som beskrivits innebär integrationen mellan domäner, och ibland i kombination med artificiell intelligens, att en stor del av ledning och samordning sker i realtid. Detta ställer enorma krav på hög rörlighet generellt men framför allt på behovet av ledningsöverlägsenhet jämfört med motståndaren. Med ledningsöverlägsenhet menas att kunna integrera och samordna alla domäner för att uppnå en effektiv bekämpningskedja.

Ledningsbehoven vid en krigföring i högt tempo innebär ökade krav på att underrättelsetjänsten kan upptäcka, bedöma och leverera måldata för högvärdiga mål. Det krävs dessutom metoder och resurser för att utvärdera om bekämpningen får avsedd effekt, och om inte, föreslå nya målsättningar. För att lyckas med detta har det därför debatterats i vilken mån det kommer att krävas en ökad grad av autonoma system som exempelvis stöds av någon form av artificiell intelligens.

2.1. Spridning och framskjuten ledning

Att eftersträva och uppnå mindre storlek på staber och ledningsplatser innebär positiva fördelar avseende rörlighet, logistik och fotavtryck, som i sin tur innebär en ökad möjlighet att uppträda dolt. Mindre storlek på staber förenklar dessutom skyddet av stabsplatsen, inklusive maskering och kamouflage. Utmaningen med staber med en mindre bemanning blir dessvärre att upprätthålla den fysiska uthålligheten samt att uppfylla den med kompetens inom samtliga funktioner och

⁸ Mattis, Jim & Bing, West. 2019:103. *Call Sign Chaos: Learning to Lead*. Random House.



domäner, särskilt staber på högre ledningsnivåer. På lägre ledningsnivåer torde hjälp av användarvänliga ledningsstödsystem med beslutsstöd kunna utgöra viktiga hjälpmedel, men det förtar inte behovet av bredd på kompetens inom staben. Detta kräver dock att samtliga ledningsnivåer har förmåga att bidra med nödvändig och skalbar information till lägesbilden.

Ett sätt att anpassa stabers storlek är att göra dem skalbara och modulära. Detta skulle innebära en ökad flexibilitet utifrån rådande situation och konfliktgrad vilket är av särskild betydelse för att snabbt kunna öka eller förstärka ledningsförmågan i tid och rum. Detta är av särskild betydelse i och med Sveriges Natomedlemskap, dels beroende på att olika länder bidrar med olika ledningsförmågor som Sverige behöver förhålla sig till, och dels då Försvarsmaktens utökade operationsområde innebär större ledningsavstånd. De större avstånden och högre tempot ställer i sin tur nya och ökade krav på ledningsförmågan och uthållighet.

De ökade kraven på ledningsförmåga kan till viss mån underlättas genom att staber delas upp i ett antal mindre enheter som är sammankopplade i ett nätverk av ett flera främre, mellersta och bakre ledningsplatser som i sin tur kan stödjas med ett förberett antal ledningsnoder, fasta eller flyttbara. Förberedda noder och skalbara, modulära staber ger möjligheten att kunna "hoppa bock" med ledningsresurser, både i tid och rum, vilket i sin tur minskar risken för ledningssvackor. Ett utökat "ledningsnät" innebär även att bakre ledningsplatser agerar som stöd (*Reach-Back*) och kan successivt förstärkas över tid och behov. Detta ställer nya krav på tekniska lösningar, exempelvis moderna och relevanta stabs- och ledningsplatser.

2.2. Behovet av taktisk ISR-förmåga

Det transparenta stridsfältet ställer ökade krav på mängden underrättelse-, övervaknings- och spaningsresurser,⁹ särskilt på taktisk nivå där ledningstempot är som snabbast. Detta kommer särskilt i åtanke utifrån erfarenheter från Ukraina med dess stora mängd obemannade farkoster för spaning och övervakning. Kommersiella mindre drönare begränsas av sin korta räckvidd samt att de är känsliga för störning, även om teknikutvecklingen visar på att räckvidden utökas successivt. Det krävs med andra ord även andra typer av inhämtningsförmågor, framförallt inom telekrigområdet. Inhämtning inom rymd- och cyberdomänen kan många gånger ske på högre ledningsnivåer och som *Reach-Back* men behöver kunna bearbetas och samordnas på taktisk nivå. Nackdelen med dessa discipliner är att de är tämligen tekniktunga och kompetenskrävande samtidigt som störförmågan utvecklas i allt högre takt.

Det kriget i Ukraina om något har visat är att det inte finns någon enskilt överlägsen inhämtningsdisciplin, utan att det är kombinationer av discipliner och förmågan att anpassa inhämtningen utifrån rådande begränsningar och behov som är nyckeln till framgång. Exempelvis framträder inhämtning av akustisk och

⁹ Intelligence, Surveillance, Reconnaissance (ISR)



termisk information allt mer som en framgångsfaktor, bland annat då det kan ske från praktiskt taget vilken plattform som helst, inklusive drönare, samt att sensortekniken här är mer motståndskraftig mot störningar. Även om Ukraina kontinuerligt uppdaterar sina ledningsstödsystem finns det utmaningar med att samordna och integrera information från olika inhämtningsdiscipliner.

Med dagens teknikutveckling har Försvarmakten en ökad möjlighet att pröva och lära sig mer om att nyttja taktiska ISR-resurser på stor bredd då både kvaliteten och kostnaden för obemannade farkoster, akustiska sensorer och kommersiella satellittjänster sjunker. Därtill kan Sverige utnyttja den inhemska utvecklings- och produktionskapaciteten. Tempot i teknikutvecklingen gör att det inte går att invänta en helhetslösning, utan lärandet och införandet av olika sensorer och hur de bäst kan användas måste ske inkrementellt.

2.3. Bekämpningskedjor – The Kill Web

Att ha en snabbare bekämpningskedja än motståndaren innebär möjligheten att slå till först mot högvärdiga mål. En degradering av motståndarens delförmågor leder förhoppningsvis till att motståndarens ledningsförmåga minskar. Med andra ord finns det en fara med att fokusera på enskilda (högpresterande) system istället för förmågan till ledning och samordning, vilket är avgörande för att optimera bekämpning i tid och rum samt är mycket tids- och resurskrävande att bygga upp när den väl är bekämpad.

Erfarenheter från kriget i Ukraina visar att både Ryssland och Ukraina har olika styrkor och svagheter avseende bekämpningskedjor. Ukrainas främsta styrka ligger i att prioritera ledningsförmåga, bland annat genom att kontinuerligt utveckla ledningsstödsystemet *Delta* samt att prioritera tempo och att få ut information (push-principen) före skydd av information. Då tillgången till ammunition har blivit mer begränsad för Ukraina ökar behovet av att kunna lokalisera högvärdiga mål på minutbasis. Detta har blivit en utmaning för båda sidor då de har lärt sig att kontinuerligt omgruppera enheter som utsätts för bekämpning.

Ytterligare en utmaning med det transparenta stridsfältet är att det innebär att en stor mängd information behöver hanteras och göras begriplig för att snabbt kunna fatta avvägda beslut. Detta är ett perspektiv på ledningsöverlägsenhet, att veta vilka resurser som gör störst nytta var, när och eventuellt hur. Då teknikutvecklingen allt mer möjliggör information och underrättelser från flera domäner blir beslut i multipla bekämpningskedjor allt mer komplexa. Denna komplexitet har beskrivit ett behov av att gå från bekämpningskedjor (*Kill Chain*) till bekämpningsnätverk (*Kill Web*) eftersom underrättelser, stridsinformation och bekämpningssystem interagerar och stödjer varandra i både tid och rum.

För att lyckas med snabba bekämpningsnätverk har artificiell intelligens beskrivits som en väsentlig framtida komponent. Inte att förglömma är att ett effektivt bekämpningsnätverk måste bygga på personalens kompetens och en organisation med kreativa och handlingskraftiga chefer. Oavsett hur utvecklingen



av artificiell intelligens kommer att te sig är det högst sannolikt att det blir problematiskt att försvara sig mot en kvalificerad motståndare som använder AI i sitt beslutsstöd om den egna organisationen inte använder AI. Hur automatiserat beslutsstödet sen ska vara blir en debatt som kommer att pågå under många år framöver. Oavsett grad av automatisering visar teknikutvecklingen på ett ökat behov av ledningsstödsystem som har inbyggda beslutsstöd med enkla och tydliga alternativ för beslutsfattare, inklusive alternativ när sensorer eller bekämpningssystem av någon anledning faller bort.

2.4. Lägesbild och visualisering

Komplexiteten med den ökade tillgången till information från olika domäner och ledningsnivåer innebär ökade möjligheter men också nya utmaningar med att tillgängliggöra informationen på lättbegripligt sätt. Erfarenheter från Ukraina visar att även om det finns ledningsstödsystem som kan presentera geografisk information med valbara lager av underrättelser eller information om egen verksamhet finns det exempelvis viss information som bäst presenteras tvådimensionellt och viss information presenteras tredimensionellt. Till detta ska läggas om informationen ska presenteras grafiskt, symboliskt eller i bild, eller alternativt som en kombination av dessa.

För stöd på stridsteknisk och taktisk nivå finns teknik som i realtid kan både förbättra bildkvaliteten och förenkla hur bilder presenteras från olika sensorer. Tekniken erbjuder även möjligheten att överlagra information från olika sensorer så att det på ett enkelt sätt går att zooma in och ut ur operationsområdet. Detta innebär att den tidigare ansedda begränsningen för att använda UAS och satellitburna sensorer i Norden på grund av väderbetingelser nu är så gott som undanröjd. Att tillgodogöra sig information är dock än så länge personalkrävande, även om artificiell intelligens är under införande för att exempelvis styra obemannade farkoster och hur dessas videobilder presenteras.

Utmaningen med att skapa en lägesbild utifrån information från alla domäner¹⁰ är att veta vilken typ av information som ska presenteras vid vilka tillfällen och för vilka beslutsfattare. Det artificiell intelligens kan erbjuda i detta avseende är att beslutsstödsystem kan lära sig att koppla informationsbehov till olika typoperationer, till olika funktioner och till olika befattningshavare där det dessutom är snabbt och enkelt att välja med olika presentationsalternativ. Inom detta område finns mycket att lära från datorspelsbranschen. Utmaningen för Försvarsmakten är att hitta en balans mellan robusta militära ledningsstödsystem, som dessutom är interoperabla, och befintlig civil teknik och kompetens, motsvarande hur Ukraina utvecklat applikationen *Kropyva* eller ledningssystemet *Delta*. Vidare behövs tydliga lednings- och lydnadsförhållanden som medger mekanismer för att sprida information om lägesbilden i cyber- och rymddomänen på taktisk, operativ och militärstrategisk ledningsnivå.

¹⁰ All-Domain Common Operational Picture



2.5. Nyttjandet av civil kommunikationsteknik

Ukraina har sedan 2014 haft en teknisk utveckling som har understötts av ett antal världsledande företag som levererar tjänster och materiel inom telekom och IT-sektorn. Här finns lärdomar att dra kring värdet av relationer mellan stat och näringsliv samt vilken roll näringslivet kan spela i totalförsvaret. En slutsats är att en variation av olika leverantörer skapar en teknisk diversitet i ledningsstödsystemen. Det innebär att olika leverantörer gör olika saker eller för den delen liknande saker men på olika vis. Detta kan vara en nackdel ur ett användarperspektiv men det bidrar även till att undvika av monokulturer inom IT.

Ur ett rent militärt perspektiv har kriget präglats av hur civil teknik nyttjas, inte minst i form av så kallade ”produkter med dubbla användningsområden” (PDA) där tekniska lösningar kan appliceras för både civila och militära syften. Nyttjande av kommersiell teknik i militär kontext har gett en god teknisk spridning, inte minst genom nyttjandet av rymddomänen, vilket i sig skapat motståndskraft och en möjlighet att försvara och hålla systemen i drift.

Fördelen med att även kunna använda kommersiella kommunikationssystem, mobiltelefonnätet i kombination med befintlig bredbandsinfrastruktur, är att det skapar redundans då dessa system i sig är relativt motståndskraftiga mot störningar. Fiberbaserade system har dessutom egenskapen att de inte har den emittering som länkbaserade kommunikationssystem har. Med 4G och 5G kan mobilnätet utnyttjas för krypterad kommunikation utan att använda mobilsamtal, vilket är särskilt viktigt för att snabbt och enkelt kunna överföra bild och video. Mobilnätet underlättar även att dela information på stor bredd vilket är av särskild vikt vid högre konfliktnivåer och mobilisering.

Lärdomen för Försvarsmakten är att hitta en balans mellan informations-tillgänglighet och informationssäkerhet, särskilt om utvecklingen går mot att i högre grad utnyttja kommersiell kommunikationsteknik, inklusive 4G, 5G och satellitkommunikation. Därtill har kriget lyft frågan om säker anskaffning där osäkra kommersiella lösningar kan leda till oönskade effekter. Ett sådant exempel är läckage av geografisk data. Lärdomarna visar dessutom på vikten av att omhänderta civila resurser för att kunna hålla högt tempo utan att ge avkall på cybersäkerhet.

En annan lärdom för Försvarsmakten är att hitta en balans mellan militära ledningsstödsystem och kommersiella kommunikationssystem för att skapa bästa möjliga ledningsredundans. Detta gäller även lagringstjänster och huruvida dessa ska vara molnbaserade eller inte. Militära molnbaserade lösningar är under utveckling och Försvarsmakten behöver utforska dessa möjligheter.

Det ukrainska ledningsstödsystemet *Delta* brukar särskilt lyftas som ett intressant exempel då systemet har en molnlösning och med servrar placerade utomlands vilket gör det omöjligt att bekämpa systemet fysiskt i Ukraina. Ledningsstödsystemet fungerar mer som en social mediaplattform än som ett



traditionellt system. Uppkoppling kan ske från en uppsjö av plattformar och autentiseringen använder i hög grad telefonen eller datorns egna system där användaren själv konfigurerar sin roll i systemet. Principer om förtroende kommer i fråga när system byggs på det här viset, och förlust av hårdvara som är en del av systemet är ett problem som behöver hanteras.

2.6. Slutsats – fail fast, fail early!

Den negativa omvärldsutvecklingen i kombination med teknikutvecklingen ställer särskilda krav på Försvarsmakten att både kunna växa, utvecklas och integreras i Nato samtidigt. Det kriget i Ukraina har visat, bortsett från att utvecklingen går snabbt, är att fungerande lösningar snabbt måste kunna anskaffas och produceras i tillräckligt stor mängd. Det behöver dessutom finnas en stor och flexibel utbildningsorganisation för att lösningarna ska kunna förbandssättas för att nå verkan. Dessvärre är väl utarbetade anskaffningar av nya materielsystem och uppbyggnad av nya förmågor mycket tidskrävande. Som tidigare har beskrivits innebär dessa långa ledtider en betydande risk med tanke på omvärldsutvecklingen och den snabba teknikutvecklingen. Förmågor och teknik kan snabbt bli obsoleta samtidigt som Försvarsmakten riskerar att missa chansen att lära sig nya förmågor. Denna risk är inte unik för den svenska Försvarsmakten utan många länder står inför samma svåra val.

Den lösning som diskuteras inom Nato för att hantera ovanstående risker är att ju snabbare en försvarsmakt prövar nya saker och lär av sina misstag, desto mindre allvarliga blir konsekvenserna av felaktiga beslut. För tillfället är varken Sverige eller Nato i en högentensiv konflikt och det finns därför ett tillfälle att lära sig och misslyckas i en säker miljö tillsammans med våra allierade och partnerländer. Men för att lyckas med detta behöver Försvarsmakten skapa en ny syn på risktagning, inklusive synen på informationssystem och säkerhetsskydd. Istället för riskaversion behöver begrepp som innovation, kreativitet och erfarenhetsanalys stå i centrum. Krigsförband, skolor och centrum behöver vara en aktiv del av experimentverksamhet och prov-och-försök där gränstorna mot industrin sker mer interaktivt och parallellt än sekventiellt.

Lärdomen för Försvarsmakten är behovet av en tillräckligt anpassningsbar organisation som har mandat och kapacitet att kontinuerligt utveckla tekniska lösningar med en kortare beslutscykel än motståndaren. Utöver en utvecklad erfarenhetshantering i Försvarsmakten behöver även industrin, akademin och andra försvarsmyndigheter vara en naturlig del av Försvarsmaktens skolor och centrum enligt *triple-helix* modellen. Detta kan förhoppningsvis leda till att gränserna mellan utbildning, utveckling, erfarenhetshantering och innovation suddas ut och där olika kompetenser både stödjer och utmanar varandra. Den svenska kulturen och mentaliteten med entreprenörsanda borde vara särskilt gynnsam för en sådan lösning och som i sin tur förhoppningsvis leder till en god förmåga att genomföra multidomänoperationer.



3. Framtidens operationskonst

*"The basic cognitive skill for dealing with surprise is creative thinking since only this type of mental activity can improvise effective solutions."*¹¹

Som beskrivits i de två föregående kapitlen finns det ett antal motsägelsefulla trender inom förändringen av krigföringen. Dessa utmaningar behöver inte enbart lösas av Försvarsmakten utan även av våra allierade i Nato, där olika försvarsmakter har olika styrkor och svagheter som behöver kunna hanteras för att skapa en gemensam avskräckande helhet. Integration och anpassningsförmåga möjliggör för Försvarsmakten att tillsammans med våra allierade bedriva operationskonst utifrån önskvärd målbild.

3.1. Behovet av enkelhet i en allt mer komplex värld

För att Försvarsmakten ska kunna bedriva operationskonst i ett högre tempo än motståndaren behöver beslutfattare övas och tränas i att samordna militär verksamhet, i alla domäner, miljöer, och ledningsnivåer, med icke militär verksamhet. Dagens teknikutveckling möjliggör att bedriva multidomänoperationer i högre grad än tidigare. Därmed behöver avancerade tekniska system inom främst cyber- och rymddomänerna och informationsområdet tillgängliggöras snabbare och på större bredd inom totalförsvaret.

Utvecklingen av avancerade tekniska system visar möjligheten att kunna analysera, presentera och visualisera en gemensam lägesbild som omhändertar information från alla domäner. Teknikutvecklingen möjliggör även förenklade och anpassningsbara beslutsstöd för att uppnå ett högt beslutstempo. Försvarsmakten behöver därför övergå mot en mer mjukvaru- och applikationscentrerad teknik istället för plattforms- och nätverksbaserade systemlösningar. På sikt behöver utvecklingen sannolikt även gå mot helt datacentriska tekniklösningar som är helt oberoende av såväl applikationer som plattformar.

3.2. Operationskonst och decentraliserat beslutsfattande

Operationskonst är normalt sett inte teknikdriven, men den operationskonst som kan bedrivas är alltid teknikberoende. Exempelvis är kunskapen om operationsmiljön, inklusive motståndaren och andra aktörer, en nödvändighet för bedrivandet av operationer. Dagens moderna teknik medför nu ökade möjligheter att presentera och visualisera valbar och anpassningsbar information på samtliga ledningsnivåer. Avancerad teknik ger med andra ord nya möjligheter i att uppnå god insikt, kunskap och förståelse för den operativa helheten hos alla chefer och hur deras egna funktioner och ansvar passar in i denna, vilket är en

¹¹ Finkel, Meir. 2011:100. *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield*. Stanford Security Studies.



framgångsfaktor för en gemensam operation. Detta lägger grunden till uppdragstaktik och uppdragsdisciplin med förmåga att snabbt ta ansvar och initiativ. För att kunna utnyttja denna möjlighet behöver handlingskraftiga och kreativa chefer ha öppna mandat med tydliga strategiska och operativa målbilder. Denna utveckling behöver även speglas i både doktrin och organisation.

Kriget från Ukraina har visat vikten av att kunna kombinera olika förmågor för att nå effekt på samtliga, taktiska, operativa och strategiska nivåer som med begränsade resurser kan orsaka strategiska dilemman. Den ökade tillgången till information ger möjligheter att exploatera svagheter hos motståndaren inom alla domäner och ledningsnivåer. Exempelvis har bekämpning av strategiska mål, såsom central infrastruktur, tidigare krävt målmedvetna, noga planerade insatser med strategiska resurser. Nu kan handlingskraftiga och kreativa chefer på lägre nivå med offensiv cyberförmåga eller tillgång till drönarteknik också genomföra denna typ av insatser. Slutsatsen är att dessa möjligheter och utmaningar behöver omhändertas doktrinärt av en välutbildad och kompetent organisation som kan exploatera dessa tankegoods utan att ge avkall på innovation och anpassningsförmåga. För att lyckas med detta behöver Försvarsmakten både ett bredare utbud på utbildning och kunna rekrytera nya kompetenser till myndigheten.

3.3. Multidomänoperationer – en resa in i framtiden

Kriget i Ukraina har visat på hur cyber- och rymdförmågor har kompletterat och förstärkt förmågorna i de tre fysiska domänerna land, sjö och luft. Detta har skett på ett mer spontant sätt snarare än på en förmåga att samordna operativa resurser för att nå avgöranden. Slutsatsen är att avancerad teknik inte nödvändigtvis får önskad effekt i operationskonsten om inte organisation och doktrin också utvecklas i ett sammanhängande system av system. Därför utvecklar Nato nu konceptet för multidomänoperationer (MDO) där den bärande idén är att samordna (*orchestrate*) all militär verksamhet, i alla domäner, med icke militär verksamhet (*synchronise*). Där igenom ökar möjligheten att skapa efterfrågade effekter i de virtuella, kognitiva och fysiska dimensionerna i relevant tempo.

Den framtida operationsmiljön och de operationskoncept som formaliseras i multidomänoperationer kan upplevas som teknikdriven men innebär främst en kulturell omställning för hur krigföringen kan bedrivas. Detta ställer nya krav på inte bara våra soldater, sjömän och officerare, utan på alla som verkar inom ramen för totalförsvaret. Organisation, förvaltningsprocesser, utbildning, och ledarskap måste anpassas för att möta dessa krav.

I och med Sveriges Natomedlemskap behöver vi inte ta oss an dessa utmaningar ensamma. Istället är det av vikt att låta utvecklingen ske inkrementellt, det vill säga att börja med de viktigaste funktionerna för att därefter göra successiva tillägg och förändringar. Genom att kontinuerligt stödja utvecklingen med värdering och erfarenhetshantering kan Sveriges och alliansens militära förmåga utgöra en trovärdig och sammanhängande helhet som kan hanterar framtida utmaningar.



I framtagandet av detta underlag har Försvarsmakten fått stöd av Totalförsvarets forskningsinstitut och Försvarshögskolan samt samverkat med Försvarets materielverk och Myndigheten för samhällsskydd och beredskap.

- o0o -

Detta underlag har föredragits i ÖB beslutsråd varvid ställföreträdande chefen för försvarsstaben, ställföreträdande chefen för operationsledningen och chefsjuristen beretts tillfälle att yttra sig.

- o0o -

Denna rapport har beslutats av generallöjtnant Carl-Johan Edström. I den slutliga handläggningen har deltagit senior analytiker Michael D. Aust, analytiker Stefan Cako, analytiker Sofia Trygged, analytiker Maximilian Richter och som föredragande sektionschef Emma Söderström.

Carl-Johan Edström

Chefen för operationsledningen

**Sändlista (huvuddokument samt bilaga 1 och 2)**

Regeringen (Försvarsdepartementet)

För kännedom

Försvarsutskottet	FöU
Sammansatta utrikes- och försvarsutskottet	UFöU
Riksdagens utredningstjänst	
Riksrevisionen	
Finansdepartementet	
Utrikesdepartementet	
Försvarets materielverk	
Fortifikationsverket	
Försvarets radioanstalt	
Kustbevakningen	
Myndigheten för samhällsskydd och beredskap	
Totalförsvarets plikt- och prövningsverk	
Totalförsvarets forskningsinstitut	
Ekonomistyrningsverket	
Försvarshögskolan	
Statskontoret	
Rymdstyrelsen	
Luftfartsverket	
Sjöfartsverket	
Vinnova	
Polismyndigheten	
Säkerhetspolisen	
Post- och telestyrelsen	
Svenska kraftnät	
Trafikverket	
Transportstyrelsen	
Myndigheten för psykologiskt försvar	
Myndigheten för totalförvarsanalys	
Fortifikationsverket	
Tullverket	

För kännedom inom Försvarsmakten

ÖB, GD

REV, FLYGI, SÄKINSP, FIHM, FST, OPL, MUST

AST, LG, I 13, I 19, I 21, K 3, K 4, P 4, P 7, A 8, A 9, Lv 6, Ing 2, T 2,

SWEDEC, SkyddC, MSS

MS, 1.ubflj, 3.sjöstriflj, 4.sjöstriflj, Amf 1, Amf 4, MarinB, SSS

FS, F 7, F 16, F 17, F 21, Hkpflj, LSS

MR Syd, MR Väst, MR Mitt, MR Norr, P 18, HvSS

FMLOG, FMTS, FömedC

MHS K, MHS H, FM HRC, LedR, FMTIS, FMUndSäkC, SOG