ISTAR 2.0

Hur öppna källor, lägre taktisk signalspaning och obemannade farkoster tillsammans bildar ett dödligt nätverk.

av Michael Winberg

Résumé

Recent conflicts, particularly in Ukraine, have demonstrated a significant shift in how intelligence, surveillance, target acquisition, and reconnaissance integrate with combat effects at the tactical level. The proliferation of unmanned systems, open-source intelligence (OSINT), and lower-level signals intelligence has increased sensor density and reduced the time between detection and engagement. This article argues that these developments represent an emerging form of ISTAR 2.0 at lower tactical levels, characterised by distributed, partially decentralised targeting networks, or "kill webs," that operate across multiple domains.

DE SENASTE ÅRENS krigföring har visat för världen hur kommersiella farkoster, hemmabyggda telekrigssystem, sociala medier och digitala plattformar inte bara kan korta ner en verkanskedja, utan också bygga ett motståndskraftigt verkansnätverk där sensorer kopplas samman med verkansenheter sömlöst. Kommersiellt tillgängliga drönarsystem, improviserade telekrigssystem, öppna källor och digitala plattformar har tillsammans bidragit till att kraftigt reducera tiden mellan upptäckt och bekämpning. Utvecklingen har lett till ett tillstånd som kallas för det transparenta slagfältet. Begreppet används för att beskriva hur sensortätheten i Ukraina har lett till att större truppsammandragningar eller ledningsplatser omöjliggjorts då de upptäcks omgående och bekämpas. Samtidigt är det även bevisligen så att sensortätheten inte har inneburit att respektive krigförande part har undgått att missbedöma det taktiska läget eller för den delen misslyckats med vissa operationer.[1] Det kommer sannolikt även vara gällande i framtiden där valet att ta en strid alltjämt kommer innebära att chefen tar en risk oavsett hur detaljerad lägesbilden anses vara.[2]

Även om det existerar en konsensus kring att slagfältet är transparent, finns det utrymme för att diskutera vilken typ av klarhet som vi menar och vilka utmaningar som kvarstår att hantera för att verkligen uppnå ett genomskinligt slagfält.[3] I synnerhet att transparensen skiljer sig åt mellan domänerna. När det transparenta slagfältet nämns i diverse artiklar handlar det främst om det visuella, det vi själva kan observera, uppfatta och därmed skjuta på. Vilket inte är konstigt i och med att vi är varelser som baserar vår uppfattning om världen på det vi kan se, samt att det är just det visuella vi får ta mest del utav från kriget i Ukraina genom diverse videoklipp som sprids på sociala medier.

Mängden drönarsystem innebär en utmaning att knyta samman sensorn med skytten (sensor-to-shooter). Därutöver kan vi lägga till en rad olika telekrigssystem för att upptäcka och skydda sig mot drönare, system

som i vissa fall är kritiska för att överhuvudtaget överleva. Därtill har ukrainska förband på lägre nivå dedikerade specialister för att genomföra inhämtning via internet för att i såväl cyberdomänen som i den fysiska världen leverera någon form av effekt mot ett identifierat mål.

Intelligence Target Acquisition Surveillance and Reconnaissance (ISTAR) samordnar underrättelse- och övervakningsresurser inom flera domäner för att leverera verkansinformation samt bidra till en gemensam lägesbild. Även om det vanligtvis pratas om JISR (Joint Intelligence, Surveillance and Reconnaissance), det vill säga att målsökningsfasen är outtalad, är det just att hitta mål som är av intresse i kriget. Försvarsmakten valde att under 2008 frångå ISTAR som begrepp till förmån för JISR som sedermera kom att bli en process baserad på särskilda förband på operativ nivå. Chefen på lägre taktisk nivå blev inte längre den primära mottagaren och delgivning av information blev mer restriktiv. Därför är ISTAR ett mer träffande begrepp än JISR när vi talar om en integrerad underrättelse- och verkansprocess på lägre taktisk nivå, där chefen är primär mottagare och information delges brett.

Information hämtad från öppna källor (så kallad open source information/intelligence – OSINF/OSINT)[4] har bevisligen haft en påverkande roll i ryska angreppskriget mot Ukraina där metoder och tekniska hjälpmedel som tidigare användes av journalister nu tillämpas för att precisionsbekämpa såväl stridsställningar längs fronten som kritisk infrastruktur i de bakre områdena. Frivilligorganisationer eller löst sammansatta grupper av intresserade med begränsade resurser bearbetar öppen information, identifierar ryska ställningar och vidarebefordrar informationen till ukrainska mottagare, som sedan slår mot de utpekade målen.

Sensortätheten tillsammans med OSINT som underrättelsedisciplin kan förstås som en tidig form av ISTAR 2.0 på taktisk nivå där brigaderna och bataljonerna nu kan agera betydligt friare än förr. Samtidigt är det inte ett helt utvecklat och fullmoget koncept som kan appliceras på varje ny konflikt eller för den delen införas omgående i en svensk kontext. För att föra en meningsfull diskussion om framtidens underrättelse- och verkansprocesser behöver denna utveckling först göras synlig. Artikeln belyser därför de tekniska, organisatoriska och kulturella utmaningarna som måste hanteras för att en decentraliserad ISTAR-process ska fungera på lägre taktisk nivå. En del i det är att fortsätta öppna upp restriktionerna kring delgivning och fortsätta kämpa emot den överklassificering (och därmed överkryptering av information) som fortsatt sker inom organisationen. Här kan vi hämta inspiration från Ukraina som låter mycket av stridsinformationen vara tillgänglig för en bred massa och att den informationen färdas över internet (förvisso fortfarande krypterat).

> *Snarare är ett verkansnät gemensamt (joint) i sin utformning och kan utnyttjas för att verka mot flera mål samtidigt i olika domäner.*

Den här artikeln kommer att argumentera för att kriget i Ukraina och den pågående utvecklingen kan förstås som en framväxande form av ISTAR 2.0, som en distribuerad och delvis decentraliserad underrättelse- och verkansprocess där sensorer, analys och verkansmedel kopplas samman i ett taktiskt verkansnät. Samtidigt kännetecknas utvecklingen av att den är organisatoriskt krävande. Sammantaget skapar artikeln en inriktning för den tekniska, organisatoriska och kultu-

rella omställningen som Försvarsmakten behöver genomföra för att ta vara på tillgänglig informationsteknologi och uppnå en snabbare verkansprocess.

Från verkanskedja till verkansnät

Traditionellt har en verkansprocess beskrivits linjärt, som en kedja (kill chain) med en början och ett slut. Kognitivt har det varit ett enkelt sätt att förklara hur processen ser ut och hur den kan motverkas. Bryt en länk i kedjan och ingen bekämpning kan ske. Därefter har konceptet utvecklats till ett verkansnät (kill web), en betydligt mer robust verkansprocess där information flödar mellan flera noder i ett nätverk, vilket försvårar för en motståndare att bryta verkansprocessen. Även om en länk bryts, exempelvis genom att sambandet med ett fjärrbekämpningssystem slås ut, kan informationen ändå nå andra förband som kan ta över uppgiften.

Ett verkansnät behöver inte nödvändigtvis syfta till att en enskild effekt ska levereras mot ett enda mål i en enskild domän. Snarare är ett verkansnät gemensamt (joint) i sin utformning och kan utnyttjas för att verka mot flera mål samtidigt i olika domäner. Den flexibiliteten behöver därmed även återspeglas i inhämtnings- och målsökningsfasen.

ISTAR 2.0 – Vad är det egentligen?

Det transparenta slagfältet bygger på att det finns ett nätverk av tekniska system som kontinuerligt överför data mellan alla uppkopplade noder. Bland dessa noder finns sensorer och bearbetningspunkter som alla bidrar till en komplett lägesbild som förmedlas nedåt utifrån de informations- eller underrättelsebehov som kommunicerats, med en hög nivå av informationsskydd. Information kan oftast flöda relativt obehindrat horisontellt men blir mer restriktivt vertikalt ju längre ner i organisationen man kommer. Det åligger en chef eller stab att aktivt argumentera för sitt informationsbehov (need to know). Detta är vad som kan sägas kännetecknа JISR eller ISTAR såväl historiskt som idag.

Att bryta sig loss från ”need to know” är den delen av den kulturella omställningen som måste till för att ISTAR 2.0 ska fungera. Om information inte delges brett och omgående spelar det principiellt ingen roll hur många sensorer eller verkansdelar du har uppkopplade till verkansnätet, inte heller hur stark bearbetningskapacitet du har. Informationen riskerar att fastna i olika rör på lokala öar där få kan ta del av densamma, och när den väl når fram till en mottagare som behöver informationen är det troligtvis för sent.

Kännetecken

ISTAR 2.0 kan definieras som ett distribuerat, digitalt och adaptivt nätverk där spaning, målsökning, stridsfältsövervakning och verkan integreras proaktivt med OSINT, lägre taktisk signalspaning, vilket möjliggör en kraftigt komprimerad och delvis decentraliserad upptäckts-besluts-verkanskedja inom brigaden eller bataljonen. Verkan ska i den här kontexten förstås som en effekt som kan vara såväl kinetisk som kognitiv. Med proaktivt menas att det nödvändigtvis inte finns tydligt formulerade underrättelsebehov när inhämtningen sker, utan dessa kan formuleras i efterhand och besvaras ur den tillgängliga databasen då inhämtning sker kontinuerligt inom operationsområdet. Allt som registreras av sensorer eller samlas in från öppna källor bearbetas strukturerat och sparas i en databas även om den specifika informationen inte svarar mot en specifik fråga där och då. Det kan lika gärna

vara först i efterhand som det framträder ett mönster som flaggas automatiskt av en stor språkmodell (Large Language Model – LLM).[5] Därutöver delges informationen brett till alla noder då det är viktigare att informationen når rätt mottagare i tid än att den skyddas från obehöriga (responsibility to share).

Det hela kännetecknas av vad som enklast kan sammanfattas som sensorpluralism. Där en kombination av traditionella militära och kommersiella sensorer knyts ihop med inhämtning via öppna källor. Eftersom det är viktigt att informationen når fram i tid kan även civila kommunikationsnätverk för 4G och 5G nyttjas likväl som civila molnlösningar för att förenkla delgivning. Det senare möjliggör för den militära kommunikationen att gömma sig i existerande infrastruktur och försvåra för fientlig upptäckt samt bekämpning.[6] Upplägget tillåter förband på lägre taktisk nivå att själva identifiera och bekämpa mål inom hela verkansspektrat inom sitt operationsområde utan att förbruka högre chefs resurser, vara beroende av att högre stab ska hörsamma deras informationsbehov eller vara uteslutande beroende av militära sambandsnät för såväl kommunikation som inhämtning.

> *Däremot kräver det en kulturell omställning likväl som att tekniska förutsättningar för att överföra data obehindrat mellan olika noder finns på plats.*

ISTAR 2.0 bör i det här avseendet inte, som nämndes i inledningen, förstås som ett färdigutvecklat system utan som ett framväxande koncept där teknisk integration, kompetens och organisatorisk anpassning är avgörande faktorer för hur väl konceptet kan användas i en svensk kontext. Konceptet bygger inte på att det finns obemannade system som inhämtar, utan ska ses som plattformsneutralt där alla typer av sensorer har en naturlig plats. Däremot kräver det en kulturell omställning likväl som att tekniska förutsättningar för att överföra data obehindrat mellan olika noder finns på plats. Vilken typ av transmissionsmedium som används kommer givetvis påverka hur snabbt information kan föras från en sensor till en verkansenhet. Med det sagt är det inte heller ett krav att all data flödar i samma hastighet, utan verkligheten kommer kräva att det finns tydliga prioriteringar kring vilken data som har företräde. Den formen av djupare tekniska analyser och hur prioriteringen ska hantera proaktiv inhämtning ligger däremot utanför den här artikelns omfång och fokus.

Begreppet ISTAR kan i sig betyda olika saker, ibland är det en process och ibland är det ett förband med de specifika förmågorna. I Sverige har vi efter en utredning och studier under tidigt 2000-tal valt att döpa om ISTAR till JISR. Oaktat vad vi väljer att kalla det är syftet att konceptet inte ska vara domänavgränsat eller enbart en teknisk produkt. För den delen ska det inte heller ses som nationsavgränsat, utan i en Natokontext finns det självklart fördelar med att se det hela som CJISTAR. Fokus ska ligga på att tillse att förbanden på lägre taktisk nivå får sina behov tillgodosedda och att dessa inte överskuggas av högre stabs upplevda behov av att visuellt se hela slagfältet, vilket i förlängningen riskerar att leda till detaljstyrning. Det vill säga att falla i samma fälla som befälhavare under Vietnam-kriget föll i när de försökte styra striden från helikoptrar, eller under Afghanistan- och Irak-eran där befälhavare försökt detaljstyra striden från ett videoflöde från en större drönare.[7]

Konceptet bör inte heller förstås som en ersättning för C5ISR, utan som en evolutionär förskjutning där delar av C5ISR:s funktioner, särskilt målsökning och verkans-

integration, decentraliseras till taktisk nivå genom distribuerade sensorer, OSINT och obemannade system. C5ISR syftar till att skapa en gemensam lägesbild för att möjliggöra ledning av striden medan ISTAR 2.0 representerar en framväxande logik där denna lägesbild omsätts direkt till verkan genom decentraliserade och tidskomprimerade verkansnät.

Möjliggörare

ISTAR 2.0 kan visualiseras som ett system i tre delar bestående av ett sensorlager, ett bearbetningslager och ett verkanslager. Sensorlagret utgörs av en kombination av militära och civila sensorer, inklusive obemannade system, lägre taktisk signalspaning och öppna källor. Bearbetningslagret ansvarar för att katalogisera, analysera och kontextualisera data till beslutsunderlag, ofta med stöd av digitala ledningssystem och AI-baserade verktyg. Verkanslagret utgörs av de system som kan leverera effekt, exempelvis artilleri, fjärrstyrda farkoster, elektronisk krigföring och cyberförmågor. Dessa tre lager knyts samman av olika former av transmissionsmedium, såväl 5:e generationens mobiltelefoni som satellitbaserat internet och molntjänster.

> *Det vill säga att sensortätheten och utbudet av sensorplattformar vi ser i Ukraina har drivits fram från lägsta nivå, i stället för den mer traditionella processen där toppnivån bestämmer sig för en specifik sensortyp eller produkt.*

Det som särskiljer ISTAR 2.0 från traditionella system är att dessa lager inte är linjärt kopplade, utan sammanbundna i ett distribuerat verkansnät där data flödar parallellt mellan flera noder, såväl civila som militära, där informationstillgången styrs av ”responsibility to share” istället för ”need to know”. Detta möjliggör en kraftigt komprimerad sensor-till-verkanscykel, men ställer samtidigt krav på integration, kulturell och organisatorisk anpassning.

Utvecklingen inom kommunikationsområdet med exempelvis Starlink medger tillgång till internet och därmed tillgång till information på ett sätt som vi tidigare inte ansett vara möjligt. Vi ser också, trots att antenner och master bekämpas, att det går att upprätthålla ett relativt stabilt telefonnät, vilket möjliggör 4G/5G-täckning, vilket i sin tur innebär att den enskilda soldaten kan ha tillgång till krypterat samband, lägeskartor och liknande. Även om det innebär en viss risk vad gäller informationspåverkan genom olika kanaler medför det också att soldaten inte behöver leva i total ovisshet om vad som händer. Den så kallade ”demokratiseringen” av kriget i form av ökad tillgång till teknik och information har inneburit att vi rört oss från transformativa processer med fokus på strategisk och operativ nivå till en mer soldat-centrisk process där allt som inte leder till ökad överlevnad eller ökad verkan för individen prioriteras ner.[8] Det vill säga att sensortätheten och utbudet av sensorplattformar vi ser i Ukraina har drivits fram från lägsta nivå, i stället för den mer traditionella processen där toppnivån bestämmer sig för en specifik sensortyp eller produkt.

Komprimering av verkanscykeln

En central effekt av ISTAR 2.0 är komprimeringen av beslut-till-verkanscykeln. Genom att länka ihop obemannade farkoster och olika verkansplattformar i en fullt digitaliserad ledningsarkitektur kombineras realtidslägesförståelse med precisionsbekämpning, vilket ökar hastigheten inom

bekämpningscykeln drastiskt. I Ukraina har drönare kopplade till olika mjukvaror minskat tiden från målidentifiering till artilleribekämpning till några minuter. Ukrainska 147:e brigaden säger sig kunna precisionsbekämpa ett mål 6 minuter efter att det upptäckts av en drönare. Jag har tidigare skrivit om hur informationsstigar måste bli motorvägar (information superhighway).[9] Det vill säga att informationen inte bara måste kunna flöda snabbt i termer av antal bitar per sekund, utan även flöda parallellt i flera vägfiler och i dataformat som är enkla att bearbeta. Försvarsmakten har börjat gå i den riktningen och i exempelvis Flygvapnet börjar ATAK (Android Team Awareness Kit) leta sig ut på lägre nivåer, vilket kommer att utgöra en viktig del i att bygga en lägesbild inom försvarsgrenen. Det finns således alla förutsättningar för att Försvarsmakten ska kunna uppnå såväl snabba som robusta bekämpningsnät där alla sensorer kopplas till alla verkansdelar på samtliga nivåer.

> *Den lägre taktiska signalspaningen integreras väl med inhämtning via internet, exempelvis sociala medier, nyhetsmedia eller bevakning av nätverkstrafik.*

Det uppblossade kriget i Nagorno-Karabach öppnade upp scenen för patrullrobotar och deras förmåga som verkansdel och som propagandamedium. Kriget i Ukraina har cementerat värdet av att ha fjärrstyrda farkoster som bär en egen verkansdel såväl som en kamera, som ett komplement till större kryssningsrobotar och den mindre precisa artillerielden som inte heller kan dokumentera sin egen effekt. Självmålssökande ammunition komprimerar sensor-till-skytt-cykeln genom att integrera sensor och stridsverkan på en enda plattform, vilket gör den idealisk för bekämpning av tidskritiska mål när dessa upptäcks, med uthållig spaningsförmåga som en positiv bieffekt. Detta gäller givetvis även för de otaliga FPV-drönarna som återfinns i det ukrainska luftrummet, på marken eller till havs. Det som återstår är att sammankoppla den verkansplattformen med inhämtning via öppna källor för att ytterligare korta ner tiden mellan upptäckt och verkan, eller för den delen avgränsa vilka målområden som patrullroboten ska befinna sig i då batteritid och aktionsradie för fjärrstyrda system (på lägre nivåer ska tilläggas) fortsatt är en gränssättande faktor.

Målet är att uppnå något betydligt viktigare än fler drönare eller fler granater, en integration av sensorer, verkansplattformar, data, drönare, elektronisk krigföring och cybereffekter i ett enda sammanhängande, dödligt ekosystem. Transformationen behöver därmed inte bara vara teknologisk utan även kulturell.

Lägre taktisk signalspaning en förutsättning för god lägesbild

Lägre taktisk signalspaning utgör en form av lokal eller regional signalspaning där elektromagnetiska utsändningar (kommunikation, datalänkar, radarsignaler med mera) inhämtas och exploateras av förband på lägre taktisk nivå. Till skillnad från operativ och strategisk signalspaning kännetecknas denna av korta avstånd till målet, närhet i tid, begränsad bearbetningskapacitet och direkt koppling till sensor-till-skytt-processer, inklusive integration med obemannade system och andra sensorer inom ramen för ett distribuerat verkansnät. Det är således signalspaning som bedrivs nära fronten med organiska sensorer för att möjliggöra en god lägesuppfattning, målangivning och egen

skyddsförmåga för brigaden eller bataljonen. Närhet i tid och rum kan vara avgörande för att hinna verka eller hinna undkomma såväl upptäckt som verkan.

Den lägre taktiska signalspaningen integreras väl med inhämtning via internet, exempelvis sociala medier, nyhetsmedia eller bevakning av nätverkstrafik för att metodiskt bygga och kontinuerligt uppdatera en korrekt lägesbild. Lägg därtill fjärrstyrda farkoster och vi har goda förutsättningar att ha en bättre situationsmedvetenhet än vår motståndare i operationsområdet. Det innebär givetvis också att fienden kan nyttja samma tekniker mot oss och att vi således även behöver kontinuerligt återmata till förbandet hur vi ska skydda oss på ett sensortätt slagfält.

Sensortätheten på slagfältet

Guillaume och Néron-Bancel beskriver transparens som resultatet av en strid om informationsöverlägsenhet och att den kontinuerligt måste vinnas, skyddas och förnekas motståndaren precis som överlägsenhet i de fysiska domänerna.[10] Det vill säga att transparensen, så som vi uppfattar den, aldrig är given utan måste skapas genom såväl teknisk utveckling som taktisk finess där den ständiga medel-motmedel-cykeln kommer att påverka hur tydligt eller otydligt vi uppfattar vårt specifika operationsområde. Författarna framhåller att transparensen på framtidens slagfält kommer att vara beroende av hur mycket stater är villiga att investera i innovation för att nå tekniska genombrott.[11] Något vi bevittnar idag när stater världen över befinner sig i ett innovationsrace gentemot varandra och resurser värda flera miljarder kronor investeras i olika projekt eller demonstratorer. Vad som däremot förefaller vara bortglömt är att det fortsatt är människor som ska omsätta innovationerna till praktisk handling och att det därmed ytterst är en människa som avgör om systemet fungerar som det är tänkt.

Den ökade sensortätheten är en grundförutsättning för ISTAR 2.0, men skapar samtidigt nya krav på bearbetning, tolkning och skydd. Innan den ryska markinvasionen i Ukraina var det antagligen få som ansåg att mobiltelefonen eller surfplattan hade en roll att spela som sensor, snarare sågs de som säkerhetshot mot den operationella säkerheten och personalen skulle i det längsta undvika att ha med sig den typen av enheter ut i fält. Den här artikeln kommer inte påstå att tankesättet var fel eller att vi i nästa krig ska tillåta enheter på bred front. Däremot behöver undersöka de möjligheter som exempelvis en smart telefon medför, i synnerhet inom ramen för totalförsvar. För är det något som har kunnat observeras i Ukraina, så är det hur mobiltelefoner inte bara gör varje soldat eller medborgare till en sensor, utan de bildar även viktiga noder för informationsspridning generellt, vilket bidrar till att bygga en tydligare bild av läget och därmed bidrar till härdade bekämpningsnätverk.[12] Likväl har åren med olika ”counter insurgency”-operationer utomlands visat att även den mest rudimentära kommunikationen kan undgå upptäckt i ett annat välövervakat område.[13] Vi lärde oss att hantera den verkligheten i Afghanistan och Mali, och vi kommer att lära oss hantera den verkligheten även i framtiden. Den stora skillnaden är skala och på vilken sida av linsen man står.

Öppna källor innebär inte bara att passivt ta emot och bearbeta information, det ger även möjlighet för underrättelsebefäl att vara aktiva i sin inhämtning. Bland annat kan OSINT fungera som en brygga till HUMINT när underrättelsebefäl får kontakt med källor som aktivt kan hjälpa till att bygga en mer högupplöst bild av läget. Vilket bland annat exemplifierats under västs intervention i

Libyen där ett franskt underrättelsebefäl kunde bygga ett nätverk bestående av ca 250 informatörer som befann sig på plats i området.[14] Ska vi kunna bygga en seriös OSINT-förmåga som fungerar i krig behöver vi börja idag med att odla trovärdiga källnätverk och utveckla hållbara metoder för att vidmakthålla dessa i fred.

Samtidigt är det inte allt att ha sensorer som detekterar och sänder information över ett transmissionsmedium. Det behövs också bearbetnings- och analyskapacitet för att sätta saker i ett sammanhang, för att kunna förstå vad som händer eller är på väg att hända och fatta välgrundade beslut. Här har OSINT spelat en viktig roll i att inte bara hitta information utan också skapa kontext. Det finns ingen brist på grupper och individer som dagligen sitter och följer upp nyhetsrapportering, bild- och videoflöden eller övervakar exempelvis ryska telegramkanaler för att bygga lägesbilder samt geolokalisera grupperingar. Det senare har inte bara inneburit att den övriga världen kan följa hur kriget utvecklar sig, det har även bidragit till att bägge sidor har kunnat bekämpa ”upptäckta mål”.

> *Sensor-till-skytt-loopen (tiden mellan att ett mål detekteras och bekämpas) framstår som ett av de mest centrala måtten på militär överlägsenhet i sensortäta konflikter.*

Även om slagfältet ses som mycket transparent är det fortfarande behäftat med osäkerhet. Trots sensortätheten i luften och på marken, bearbetningskapaciteten från allmänheten och kommersiella spaningssatelliter krävs det fortsatt att en människa bedömer sannolikheten för att informationen är korrekt, eller för den delen vad det är för objekt som syns på en satellitbild. Detta innebär utmaningar då det av naturliga skäl drar ner verkanstempot i relation till nivån av osäkerhet.

Sensor-till-skytt-loopen (tiden mellan att ett mål detekteras och bekämpas) framstår som ett av de mest centrala måtten på militär överlägsenhet i sensortäta konflikter. Moderna stridssystem sammanfogar data från multipla sensorer till en enhetlig operativ bild, vilket gör att beslutsfattare kan agera inom sekunder snarare än timmar. Det i sig öppnar upp för andra utmaningar, både metodmässiga och organisatoriska.

Organisatoriska förutsättningar

I Ukraina bygger majoriteten av sensorkedjorna på luftburna farkoster. Exempelvis har ukrainska artilleribrigader en organisk underrättelsebataljon som använder bevingade farkoster för uthållig inhämtning på djupet. Manöverbrigaderna har på samma sätt en självständig uav-bataljon (eller minst ett kompani) med samma typ av uppgifter. Ledningen av de här resurserna är förlagd på brigadnivå på såväl den ukrainska som den ryska sidan.[15]

Från kompani och uppåt återfinns numera såväl sensorer som bekämpning som organiska resurser som den lokala chefen har rådighet över. Även om en brigad givetvis rent traditionellt har haft bekämpningsresurser sedan tidigare, har sensortätheten och sensorupplösningen varit betydligt sämre. Inte sällan har kvalificerade resurser fått tillföras för specifika ändamål. Idag kan brigaden äga sensorer såsom taktisk signalspaning, drönare och inhämtning via OSINT och därmed agera betydligt mer oberoende av högre stab. Detta är en markant skillnad från hur vi sett på bekämpningsprocessen tidigare och framför allt hur vi dimensionerat underrättelsesektionen på en brigad.

Det finns givetvis fler faktorer att ta hänsyn till i sammanhanget, främst att ledningsplatserna behöver bli mindre (såväl fysiskt som spektralt) och att olika faser i ett krig ställer olika krav på hur staber bör vara organiserade. Jag säger därmed inte att en underrättelsesektion på en brigad eller i ett basområde kan se likadan ut i början av ett krig som tre år in i detta. Däremot vill jag påstå att vi kan tänka om drastiskt kring hur sektionerna utformas och vilka kompetenser som de olika befattningshavarna behöver ha. Oavsett om vi lägger resurserna under underrättelsesektionen eller genomförandesektionen ställer det krav på att individer är tränade för att dels hantera en bred katalog av sensorer, dels för att på sektionen inhämta samt bearbeta extern information i ett högt tempo. Här har givetvis AI-understödda bearbetningssystem en roll att spela, men som jag kommer att återkomma till senare i artikeln, det innebär inte att det enskilda underrättelsebefälet blir obsolet utan snarare tvärtom.

Data är inte underrättelser eller kunskap

Den ökade datatillgången i både mängd och hastighet riskerar att skapa en illusion av förståelse. Det finns en reell risk att informationen från en sensor övertrumfar underrättelsebefälets bedömning när chefen avgör vilket handlingsalternativ som ska realiseras eller att mängden information helt enkelt leder till en kognitiv överbelastning.[16][17] I praktiken ökar snarare kraven på tolkning, validering och kontextualisering. Det s k transparenta slagfältet är i verkligheten en ofullständig och ibland vilseledande konstruktion.[18] Det faktum att data kan samlas in är inte synonymt med att förstå en motståndares strategiska mål, motivationer eller psykologiska drivkrafter. All underrättelse är i viss mån en välgrundad gissning som kontinuerligt måste valideras. Ukrainas Kursk-operation 2024 illustrerade detta då det, trots massiv ISR, länge var oklart vad som faktiskt var på väg att ske och ukrainska styrkor lyckades överraska ryska förband samt ta sig in på djupet av ryskt territorium. Trots sina fördelar kommer transparens alltid att begränsas av mänskliga tolkningsfel samt fiendens åtgärder genom maskering och vilseledning. Framsteg inom ISR leder parallellt till utveckling av medel för att skapa ogenomskinlighet: signaturanpassning och störning av sensorer i hela det elektromagnetiska spektrumet.

> *Mer artificiell intelligens (AI) kommer inte att vara lösningen på problematiken.*

Framgångarna med OSINT i Ukraina har skapat förväntningar på att det är oumbärligt i framtida konflikter, men framgången kan vara kortvarig på grund av en mångfacetterad motoffensiv mot disciplinen. Både statliga och icke-statliga aktörer lär sig kontinuerligt att aktivt motverka inhämtning via olika former av publika källor. Bland annat genom att aktivt strypa tillgången till olika medieplattformar och att på olika sätt försöka kontrollera narrativ så att all annan information dränks i informationsflödet.

Mer artificiell intelligens (AI) kommer inte att vara lösningen på problematiken, även om AI kan avlasta och hjälpa till med mycket av datahanteringen. Min uppfattning är att AI förväntas vara en gyllene kula som ska leda till snabbare och mer korrekta beslut. Men för att AI ska kunna vara den katalysator som organisationen önskar måste det till TTP:er (taktik, teknik, procedurer) och personal med rätt kompetensprofil för att hantera den data som förs in i systemet likväl som att tolka den data som tas ut ur systemet. Även om Ukraina lyfts fram som ett

land med hög teknisk mogenhet och moderna ledningsstödssystem, sitter det fortfarande människor som varje dag föder systemet med information från exempelvis drönarvideos. Den data som presenteras på olika sätt efter att ha bearbetats av AI, kommer inte bli av högre kvalité än vad exempelvis stabsassistentens förmåga att strukturera informationen vid input.[19] Det vill säga att det kommer fortsatt vara kritiskt att rekrytera och utbilda kompetenta individer för att bemanna olika assistentbefattningar i organisationen, samt att dessa kontinuerliga vidareutbildas i takt med att ledningsstödssystem införs och utvecklas. Det är av vikt för att kunna bygga en tilltro till underlaget för att militära chefer ska våga fatta beslut.

Vi måste inte heller förledas av att en utökad mängd data per automatik innebär att vi har en bättre lägesförståelse eller beslutsunderlag. Data är inte detsamma som underrättelser eller kunskap. För att uppnå kunskap behöver vi sätta data i ett sammanhang för att få kontextuell förståelse, vilket lägger grunden för att vi ska kunna få kunskap om situationen. Det är i sin tur viktigt för att vi ska kunna förstå allt vi ser och kunna (re)agera för att kunna utnyttja situationen till vår fördel. Det vill säga att även om vi idag kan träna AI-modeller att räkna ut var det är optimalt att placera ut ett radarsystem, behöver vi fortfarande ta höjd för att det är människor som fattar beslut och att dessa långt ifrån alla gånger är optimala i sig.

Det kommer inte lösa sig av sig självt

ISTAR 2.0 bygger på en innovationslogik som i grunden skiljer sig från hur Försvarsmakten traditionellt driver utveckling. Kapprustningen är ett faktum och alla stater försöker ligga i framkant, antingen genom egen utveckling eller genom att köpa in teknik från multinationella företag. Det pratas också mycket om att de militära styrkorna inom Nato behöver bli mer innovativa. Försvarsmakten är inte på något sätt ett undantag. Begreppet ”innovation” har på kort tid blivit det nya avseende ”operativ effekt” eller ”tröskeleffekt”. Det är inte min mening att vara raljant i frågan utan att rent krasst peka ut att begreppet har förlorat lite av sin betydelse, i synnerhet när det numera går att påstå att det vi egentligen menar är ”generalsinnovation” (top-down) i stället för ”soldatinnovation” (bottom-up). Givetvis finns det undantag, men införandet av experimentkontor, särskilda projekt och FMV:s ”Battle Week” tyder alltjämt på att innovationen förväntas komma från toppen, i form av stora transformativa projekt som ska revolutionera svensk krigföring. Det går tvärtemot den erfarenhetsrapportering som kommer från Ukraina där det snarare är småskaliga projekt som svarar mot specifika upplevda problem vid fronten som står för innovationen. Den bottom-up-drivna innovationen i Ukraina är inte ett sidospår, utan en förutsättning för att ISTAR 2.0 ska fungera på taktisk nivå.

Just den formen av innovation förutsätter, eller rättare sagt kräver, att det finns individer i hela organisationen som på olika sätt lägger in egna resurser i form av tid och energi (ibland även pengar) för att utforma lösningar. Den innovationen kommer sannolikt inte att levereras från centrala processer eller multinationella företag, helt enkelt för att kostnadskalkylen inte går ihop. Detta innebär med andra ord att ISTAR 2.0, där OSINT tillsammans med små egenbyggda farkoster bidrar till en effektiv bekämpning, bygger på att det är enskilda individer på lägre taktisk nivå som bygger lösningarna utanför ordinarie processer och beprövad erfarenhet. Den innovativa utmaningen på central nivå blir

sedan att knyta ihop de olika lokala lösningarna och göra dem överförbara mellan operationsområden och domäner. För industrin blir utmaningen att göra små lösningar skalbara och så pass anpassningsbara att de har en rimlig chans att överleva mer än enstaka veckor. Vi behöver således inse att det ekonomiska spelet som vi vant oss vid i fred inte längre gäller. Innovationstriangeln innebär att vi inte kan bejaka de olika intressen som staten, industrin och soldaten har.

> *Soldatens intressen ska vara överordnade övriga genom att resurser i form av kapital och personal dediceras till att hjälpa fram de soldatnära innovationerna.*

Om staten ska spara pengar eller åtminstone hålla nere kostnaderna, kommer det att påverka industrin och soldaten negativt. Ska industrin ha möjlighet att plocka ut vinst och våga investera långsiktigt kommer det att ske på bekostnad av både statens ekonomi och soldatens behov av snabba lösningar. Om soldaten ska prioriteras genom snabba lösningar utifrån en begränsad tidshorisont måste det ske på bekostnad av såväl statens ekonomi som industrins krav på avkastning. Det kan tyckas vara en pessimistisk syn på vägen framåt, och det kommer möjligen möta mothugg från dem som befinner sig i någon av de centrala processerna. Samtidigt måste det här paradigmet synliggöras och diskuteras öppet om vi ska ha en chans att uppnå det vi säger oss vilja uppnå i form av en innovativ försvarsmakt där förbandets krigsförmåga står i centrum. Då är det rimligt att soldatens intressen ska vara överordnade övriga genom att resurser i form av kapital och personal dediceras till att hjälpa fram de soldatnära innovationerna.

Vad innebär det här konkret för Försvarsmakten?

Det är i kombinationen av OSINT, sensorer och bred proaktiv delgivning som ISTAR 2.0 realiseras, inte i någon enskild sensor eller plattform. Konceptet representerar en framväxande decentraliserad underrättelse- och verkansprocess driven av sensorpluralism, där alla former av inhämtning är av värde, även på taktisk nivå. Försvarsmakten behöver genomföra såväl en kulturell som en teknisk resa för att ta steget dit.

En aspekt som är väl värd att ha i bakhuvudet är just vilka individer och med vilken kompetens som man placerar var. I Ukraina förekommer det att exempelvis personer med bakgrund inom teater blir placerade för att bygga skenmål medan personer med bakgrund inom IT jobbar med olika ledningsstödssystem. På samma sätt beskriver Nato hur OSINT-personal mycket väl kan ha en bakgrund som bibliotekarier eller inom informationsvetenskap. Det vill säga att det är rätt väg att gå med flera vägar in mot officersyrket för att tillse att Försvarsmakten har en så bred rekrytering som möjligt för att kunna bygga upp och bemanna en OSINT-organisation i framtiden. Ett steg i rätt riktning är att försöka utnyttja den särskilda officersutbildningen (SOFU) som ett verktyg för att hitta personer med den kompetensprofil som exempelvis Nato beskriver i sin doktrin.[20]

Fokus bör ligga på att exempelvis brigaden ska kunna fungera som en nod i verkansnätverket. Det är realiserbart under förutsättning att de organisatoriska ramarna finns i form av såväl driftpersonal av tekniska system som analytiker på lägre nivåer, och att det sker ett kulturellt skifte där bearbetad information från öppna källor erhåller samma tillit som underrättelser förmedlade från högre

stab. På så vis kan vi utnyttja det transparenta slagfältet till vår fördel och samtidigt undvika att låsa in oss i ett kognitivt beroende av visuella sensorer.

Försvarsmakten är på jakt efter innovativa tekniska lösningar för framtidens krig. Vi får inte i denna strävan bli blinda för de organisatoriska och inte minst kulturella innovationer som också måste till för att kunna slå mynt av de tekniska lösningarna. I synnerhet om vi vill hitta fungerande soldatinnovationer som kan implementeras här och nu istället för visionära generalsinnovationer som kanske aldrig hinner levereras till förbanden innan kriget är över.

Författaren är fanjunkare i Flygvapnet.

Noter

1. Garnier, Guillaume & Néron-Bancel, Pierre: *The Benefits and False Promises of Battlefield Transparency*, Ifri, Paris, 2024, s 12, *https://www.ifri.org/sites/default/files/2024-10/ifri_garnier_neron-bancel_transparency_battlefield_2024.pdf*, (2026-04-16).
2. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 16.
3. Ibid, s 16.
4. I artikeln kommer OSINT att användas som synonym för information funnen hos öppna källor, oavsett om den är bearbetad i underrättelsesyfte, publicerad i traditionell media, på sociala medier eller någon annan plattform.
5. Alenjung, Zackarias, Lindholm, Victor & Karlsson, Johan O: *Stora språkmodeller som ett stödverktyg vid militär taktisk planering – slutsatser från två tillämpade studier av stora språkmodeller,* Totalförsvarets forskningsinstitut, Stockholm, FOI-R—5852—SE, 2026.
6. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 56.
7. För vidare resonemang kring den problematiken rekommenderas boken Blaber, Pete: *The Mission, the Men, and Me*, Berkley Caliber, New York 2008.
8. Ford, Matthew: ”From innovation to participation: connectivity and the conduct of contemporary warfare”, *International Affairs* 100:4, 2024, 1531–1549, s 1536.
9. Winberg, Michael: ”Obemannade system idag och imorgon – En översikt”, *KKrVAHT*, 4. häftet 2024, s 92-109.
10. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 13.
11. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 4.
12. Ford, Matthew: ”From innovation to participation…”, s 1548.
13. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 21.
14. Pollock, John: ”People Power 2.0 How civilians helped win the Libyan information war”, *MIT Technology Review*, 20 April 2012, *https://www.technologyreview.com/2012/04/20/186647/people-power-20/*, (2026-04-12).
15. Watling, Jack & Reynolds, Nick: *Tactical Developments During the Third Year of the Russo-Ukrainian War*, RUSI, London, 2025, s 14f, *https://www.rusi.org/explore-our-research/publications/special-resources/tactical-developments-during-third-year-russo-ukrainian-war*, (2026-04-16).
16. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 29.
17. Ford, Matthew: ”From innovation to participation…”, s 1548.
18. Garnier & Néron-Bancel: *The Benefits and False Promises*…, s 51.
19. Andersson, Christer, Gustavi, Tove & Karasalo, Maja: ”Artificiell intelligens – möjligheter och utmaningar för Sveriges nationella säkerhet”, Totalförsvarets forskningsinstitut, Stockholm, *FOI Memo 6749*, 2019, s 2.
20. *AJP-2.9*, *Allied Joint Doctrine for Open-Source Intelligence*, Edition A version 1, June 2019.