Datadrivna försvarsförmågor – trender och vägval

Inträdesanförande i KKrVA avd IV den 7 december 2022
av Johan Sigholm

Résumé

It has been said that data has surpassed oil as the world's most valuable resource. However, refining constantly increasing data flows to information, and producing actionable insights, is a non-trivial process. In its ongoing transformation to become a more data-driven organization, the Swedish Armed Forces face several challenges. These include the ability to attract and retain talent within various fields of digitalization, to gradually replace conventional work methods in favor of agile development practices, and to establish robust partnerships with industry and academia to leverage such emerging technologies as AI, networked unmanned platforms, and advanced space capabilities. Internal IT-systems must also increasingly be integrated with NATO and other partner systems for data collection, processing, and dissemination. The foundation of digitalization is built on existing resources, gradual improvement, identification of achievement as well as mistakes, in a transparent and inclusive change process. Additionally, and perhaps most importantly, successful digital transformation of the Swedish Armed Forces requires long-term commitment, strong leadership, and unwavering political support. This is essential not only to define the digital path ahead, but to make continuous well-informed and balanced decisions based on knowledge of opportunities and limitations of digitalization.

JAG VILL HÄVDA att den pågående digitala transformationen är den enskilt starkaste kraft som påverkar vårt samhällsklimat i dagsläget. Vid sidan av andra så kallade megatrender som globalisering – med ökade flöden av människor, varor och kapital mellan länder – urbanisering, och en i ökande utsträckning multipolär värld, driver digitaliseringen genomgripande förändringar i interaktionen mellan människor, hur information och tjänster kan konsumeras, och våra förväntningar på vad som är möjligt att åstadkomma med givna resurser.

Trots att många experter talar om digital transformation, så verkar få förstå, eller kanske ens bry sig om, dess verkliga innebörd och vilka möjligheter digitalisering faktiskt innebär. Det är abstrakta begrepp som diskuteras, ofta av akademiker och tekniker, eller politiker som vill framstå som moderna och utvecklingsorienterade. Jag menar att det som få har tagit till sig är det faktum att digitalisering inte handlar om att köpa in en massa ny avancerad IT-utrustning till oss tekniknördars stora förtjusning, eller för den delen att göra drastiska förändringar i hur vi bedriver verksamheter idag. Digitalisering handlar i grunden om att göra det vi gör idag, fast bättre, snabbare, mer kostnadseffektivt och faktiskt även mer bekvämt. På så vis kan

tid och resurser frigöras för att lösa andra problem, eller ge oss ett utökat utrymme att engagera oss i mellanmänsklig interaktion. Digitalisering handlar alltså om rationalisering, resursoptimering, och att skapa och tillgängliggöra ny kunskap, till stöd för mänskliga beslut. Genom att arbeta smartare, mer effektivt och ha tillgång till bättre beslutsunderlag kan man helt enkelt åstadkomma mer med mindre, snabbare och med högre precision. Det är vad som ligger i den positiva vågskålen. Det finns dock givetvis utmaningar. Låt mig återkomma till dessa.

Tekniktrender

Den tekniska utvecklingen är just nu väldigt kraftig inom områden som smarta, obemannade farkoster, bearbetning av stora datamängder med hjälp av artificiell intelligens (AI), och av rymden som medium för digital kommunikation. Kommersiella aktörer dominerar här i stor utsträckning helt utvecklingen. En slags kapprustning pågår kring vem som kan lansera de kraftfullaste AI-stödda tillämpningarna, där OpenAI och dess tjänster DALL-E och ChatGPT har fascinerat, men samtidigt manat till eftertanke kring framtida utveckling, dess möjligheter och konsekvenser. Bara under det senaste årtiondet har vidare antalet satelliter som skickats upp i rymden fyrdubblats och prognoser pekar på att det år 2030 kommer att placeras närmare 2 000 satelliter per år i omloppsbana.

Genom de resulterande megakonstellationerna skapas global tillgänglighet till digitala tjänster – även i områden som tidigare var vita fläckar på täckningskartorna. Redan idag ser vi en utveckling som pekar i denna riktning genom exempel som Apples senaste mobiltelefonmodell, iPhone 14 (September 2022), som kan kommunicera direkt med satelliter i låg omloppsbana – om än med begränsad datatakt. Pågående forskning pekar vidare på att alltmer lagring och behandling av data i framtiden kommer att ske i rymden, med tekniker som så kallad ”edge computing”, vilket möjligtvis på svenska kan benämnas ”kantdatorsystem”.

Konsekvenser för militära vidkommanden

När detta skrivs rasar hårda strider mellan ukrainska och ryska styrkor kring staden Bachmut i norra Donetsk oblast, i Ukraina. Vintern är i antågande. Höstens regn och lera har givit vika för snö och kyla, med temperaturer ned mot 10 minusgrader. I princip all infrastruktur är utslagen i området, gällande såväl elförsörjning som mobil kommunikation, och kraftig störning genomförs i det elektromagnetiska spektrumet. Det är därmed utmanande att leda operationer i området. Ukrainska förband har dock uppvisat en imponerande förmåga att ta till sig av moderna, kommersiellt tillgängliga digitala verktyg.

Ledningscentraler byggs upp i källare under mark, där egna förbands position presenteras på stora skärmar – fiendens grupperingsplatser lika så. Dessa identifieras i realtid via ”appar” från observatörer, eller via drönare, där bild strömmas i direktsändning. Behovet av åtminstone enklare reservdelar, såsom rotorblad, kan fyllas på plats med hjälp av additiv tillverkning i 3D-skrivare. Genom relativt små, behändiga terminaler, donerade av den amerikanske entreprenören (och tillika världens för närvarande rikaste person) Elon Musk och hans företag Starlink, länkas lednings- och kommunikationssystem ihop. Utöver traditionella dieseldrivna generatorer tillhandahålls även elkraft från utrullningsbara solpaneler, där överskottsenergi lagras i så kallade Powerwalls – kraftiga batteripaket ursprungligen avsedda för

att ladda elbilar. Med hjälp av AI-stödd mjukvara avlyssnas radiokommunikation, tolkas i realtid till text, och bidrar snabbt till värdefulla och ofta tidskritiska underrättelser. Information utbyts kontinuerligt mellan partnerländer, vilket bidrar till att bygga en gemensam lägesbild. Utveckling av nya digitala förmågor sker agilt, där den huvudsakliga drivkraften är det existentiella hotet mot staten Ukrainas överlevnad – ett nog så kraftfullt incitament.

Med detta vill jag dock inte hävda att det är de digitala verktygen, vapnen och den avancerade behandlingen av information som i slutänden blir avgörande för Ukrainas möjligheter att besegra Ryssland militärt. Men det är sannolikt en pusselbit i de ukrainska styrkornas förmåga att försvara sig mot en numerärt överlägsen motståndare.

En historisk tillbakablick

När det gäller begreppet ”digitalisering” så får jag tillstå att det, i sig, inte är något nytt. Vissa menar att digitaliseringen av Sverige inleddes redan i samband med den framväxande datoriseringen på 1970- och 80-talen, och senare med hem-pc-reformen på 1990-talet. Försvarsområdet genomgick samtidigt en ”Revolution in Military Affairs” och under det första decenniet av 2000-talet gjordes stora ansträngningar att digitalisera försvarsmakter genom koncept som Network Centric Warfare, som inom Försvarsmakten utvecklades inom ramen för konceptet NBF – det nätverksbaserade försvaret. Trots att NBF inte lyckades nå önskade resultat om väsentligt ökad operativ förmåga på kort sikt, är grundtankarna, i realiteten, i mångt och mycket desamma som för den utveckling vi ser idag. Snabbare och effektivare beslutsfattande och ledning, baserat på tekniska system för kommunikation och informationsbehandling, där staber, förband och verkanssystem och befattningshavare länkas samman. Sannolikt var man dock med NBF ”före sin tid”, och den utbredda teknikoptimism som präglade inte bara det svenska NBF-konceptet, utan även många andra länders motsvarigheter, var inte hållbar.

Det har nu gått ytterligare ett par decennier och det är det mycket som tyder på att vi fortfarande bara befinner oss i början av den digitala transformationen. Det är en förändringsresa som kommer att fortsätta flera decennier in i framtiden. Möjligtvis ser vi dock idag en ökad förändringstakt i förhållande till de senaste två decennierna. De kommande åren kommer att innebära stora förändringar inom områden såsom molnbaserade tjänster för överföring, behandling och lagring av data, och, som jag tidigare nämnde, artificiell intelligens och en ökande användning av rymden som medium för digitala tjänster. Denna snabba utveckling, som alltså huvudsakligen drivs av kommersiella aktörer med tjänster och produkter riktade mot företag, myndigheter och enskilda individer, är viktig att bevaka, långsiktigt planera för och förhålla sig till.

Aktuella förutsättningar

Vi befinner oss i en omvälvande tid för Försvarsmakten. Den säkerhetspolitiska situationen i vårt närområde har under de senaste två decennierna gått från att präglas av lugn, stabilitet och nära samarbete länder emellan, till ett kraftigt försämrat omvärldsläge. Detta drivs, som bekant, till stora delar av Rysslands auktoritära strävanden och ambitioner att utöva inflytande över framförallt de f d sovjetrepublikerna. Ryssland har genom sitt anfallskrig mot Ukraina ensidigt förkastat den tidigare rådande regelbaserade säkerhetsordningen. Landet har uppvisat såväl stor hänsynslöshet som en

acceptans att ta omfattande risk. Detta påverkar givetvis bedömningar av Rysslands framtida agerande, även mot Sverige och svenska intressen.

En adekvat och trovärdig försvarsförmåga måste kunna upprätthållas, såväl enskilt som tillsammans med allierade, där beredskapen kontinuerligt kan anpassas utifrån olika händelseutvecklingar. Försvarsmakten har fått i uppdrag att till regeringen redovisa hur en nivå motsvarande två procent av BNP ska kunna nås, med framflyttat mål till 2026. Sannolikt behövs dock ytterligare medel för att kunna nå mål inom såväl personalförsörjningen som omfattande investeringar i bland annat nya IT-system och IT-infrastruktur för att hantera information som en strategisk resurs.

Sverige lägger samtidigt om sin försvars- och säkerhetspolitiska kurs, med en anslutning till Nato. Som medlemmar av denna allians förväntas Sverige kunna verka med militära förmågor såväl för försvaret av Sverige som för allierade. Effektivt samarbete inom alliansen kräver interoperabilitet gällande såväl processer som system, men sannolikt även att kunna dela på uppgifter och förmågor kopplade till digital informationsbehandling.

Den pågående Nato-anslutningen medför även en omfattande förändring i Försvarsmaktens ledningsstödsystem. Säker kommunikation för informationsutbyte mellan Sverige och Nato är en förutsättning för ett fungerande medlemskap. Utveckling av system i enlighet med ramverket Federated Mission Networking (FMN) är en grundpelare för att stärka Försvarsmaktens ledningsförmåga, såväl nationellt som för samverkan inom Nato. Anslutning till gemensamma Nato-system som NSWAN[1] och BICES[2] är en förutsättning för att kunna överföra och utbyta såväl öppen som hemlig information, lägesbilder och underrättelser med allianspartners.

Försvarsmakten genomför nu stora satsningar för att gå mot att bli en mer datadriven organisation. Överbefälhavaren har beslutat att takten i myndighetens digitala transformationsarbete ska ökas, i syfte att bland annat kunna upprätthålla ett informationsöverläge i förhållande till en framtida motståndare. Man utvecklar bland annat det som kallas för den ”digitala ryggraden”. Det handlar till del om att se till att utveckla kraftfullare bärarnät för informationsöverföring i landet, som samtidigt är mer robusta och resilienta – det vill säga som kan utstå påfrestelser som ett väpnat angrepp, men även snabbt kunna återgå i drift efter systempåverkande händelser. Dessa nät ska stödja tjänster som kräver överföring av stora mängder data, från exempelvis olika sensorer, och som kan hantera information med högt skyddsvärde, i hela konfliktskalan.

Digitaliseringen inom Försvarsmakten handlar även om att anamma nya sätta att arbeta, med metoder som agil systemutveckling, bland annat så kallad DevOps – där utvecklare arbetar tillsammans, och i nära samarbete med, ansvariga för drift och systemunderhåll. Försvarsmakten vill även i större utsträckning sluta utveckla sina digitala system själva utan i högre grad anskaffa dessa på en kommersiell marknad, för att senare anpassa dem utifrån verksamhetens behov.

Utmaningar och vägval

Trots Försvarsmaktens ökade anslag är resurserna trots allt begränsade. Det gäller alltså att veta vad som ska prioriteras för att lyckas med den digitala transformationen.

Om inte rätt kompetens finns bland personalen hjälper det inte att anskaffa avancerade tekniska system. Här gäller det att yt-

terligare öka Försvarsmaktens attraktivitet som arbetsgivare och i synnerhet att rekrytera (och behålla) civil personal med olika spetskompetenser. Jag vill därför betona att jag ser personalförsörjning inom IT-området som en avgörande pusselbit för möjligheten till framdrift inom Försvarsmaktens digitalisering de kommande åren.

Om verksamheten inte organiseras på ett rationellt sätt, anpassad utifrån digitalt arbete, når man inte önskad effekt. Stuprör måste kapas, eller åtminstone förses med effektiva hängrännor. Här bör Försvarsmakten sannolikt fundera på att utveckla möjligheterna för medarbetare att kunna jobba på distans – åtminstone delvis och för vissa befattningar – för att på ett bättre sätt spegla dagens civila arbetsmarknad. Detta kan man till del åstadkomma genom att anamma moderna designparadigm för cybersäkerhet som ”Zero Trust”, en strategi som förlitar sig på stark autentisering och rollbaserade rättigheter, snarare än brandväggar och skalskydd.

Om arbetssätt och metoder inte stödjer digitaliseringen når man inte effekt. Adekvat dataförsörjning är en förutsättning för att kunna arbeta med mängddataanalys, där produktion och verifiering av dataset kontinuerligt måste ske och systemutveckling gå i den takt verksamheten kräver. Samtidigt måste de använda systemen vara såväl trygga som säkra, så att gällande lagstiftning kan upprätthållas och källor skyddas mot exponering. Verksamheten måste även vara etiskt hållbar och ligga i linje med myndighetens gemensamma värdegrund.

Om digitalisering ses som ett kortsiktigt, avgränsat projekt blir förmågan inte hållbar. Nya stödjande komponenter måste utvecklas etappvis, där resultat kontinuerligt utvärderas, såväl gällande framsteg som motgångar. Förbättringar bör göras stegvis, med såväl centrala som decentraliserade tjänster, utifrån en tydlig strategi om ökad verksamhetsnytta. Såväl egna som publika molnbaserade lösningar kommer sannolikt att förekomma, men att lägga alla ägg i en och samma korg är inte en klok väg att gå. Risken finns annars att man hamnar i samma återvändsgränd som med NBF.

Om man sitter och väntar på att ett tekniskt framsteg ska ske för att dra med organisationen i digitaliseringsresan, såsom ett avancerat AI, finns risken att man blir besviken. Genom att införa förändringar gradvis, i kombination med parallella insatser inom utbildning, en successiv organisationsutveckling och ett kontinuerligt lärande från ofrånkomliga misstag och kanske oväntade framgångar, kan man reducera riskerna för att såväl övervärdera digitaliseringens betydelse på kort sikt, som att undervärdera den i ett längre perspektiv. Det kräver dock ett tydligt ledarskap i digitaliseringen, en långsiktig strategi, och en kontinuitet som för Försvarsmaktens del sträcker sig över flera kommenderingsperioder.

Om man tror att digitaliseringen av Försvarsmakten ska vara en helbrägdagörare som kommer att leverera en mirakelkur som löser alla problem så är man sannolikt fel ute. Det finns många utmaningar som en digitaliserad organisation kommer att dras med även i framtiden. Det handlar om saker som meningsskiljaktigheter, resurskonflikter och den mänskliga faktorn. En ökad interaktion med datorgränssnitt kan även skapa intrycket av att mellanmänskliga interaktioner inte längre är värdefulla. Så är givetvis inte fallet. Det är därför viktigt att alla digitaliseringsprocesser är transparenta, och inkluderande, så att ett förtroende kan byggas inom organisationen som genomgår förändringen.

Avslutningsvis så ska man heller inte glömma att Försvarsmakten är en del av ett omgärdande samhälle, som i sin tur omges av en alltmer globaliserad omvärld. Ser man på

längre sikt kommer även klimatförändringarna att bidra till ökad instabilitet i såväl vår egen som andra regioner inom Natos intresseområden, genom vattenbrist, mer frekvent förekomst av extremväder, samt den ökande strategiska och militära betydelsen av Arktis.

Att kunna göra pålitliga bedömningar av olika händelseutvecklingar får stor betydelse för möjlighet att möta dessa. Omställningen från fossila bränslen till förnyelsebar energi, och konkurrens om värdefulla naturresurser såsom värdefulla jordartsmetaller, kommer vidare att få geopolitiska konsekvenser på grund av deras centrala betydelse för digitaliseringen av såväl Försvarsmakten som det svenska samhället i stort. Detta gäller särskilt så kallade innovationskritiska metaller och mineraler, något som lyfts i det nyligen överlämnade betänkandet ”En tryggad försörjning av metaller och mineral” (SOU 2022:56). Tillgången till dessa anses i utredningen vara avgörande för teknikinnovationer inom exempelvis digitalisering och produktionen av viss försvarsmateriel. En risk som särskilt påpekas är Kinas dominerande ställning med kontroll över globala värdekedjor med relevans för totalförsvaret.

Slutsatser

Försvarsmaktens huvuduppgift kommer sannolikt även i framtiden, åtminstone inom en överskådlig tidsperiod, vara att försvara Sverige mot ett väpnat angrepp. Mot bakgrund av vad jag redovisat finns goda skäl att anta att en fortsatt digitalisering av Försvarsmakten är nödvändig för förmågan att såväl upptäcka som identifiera, analysera och möta hot mot Sverige och svenska intressen. Samtidigt blir ett Sverige, med en digitaliserad försvarsmakt, en mer effektiv och eftertraktad samarbetspartner inom Nato samt med övriga nationella och internationella samarbeten inom underrättelse- och säkerhetsområdet.

Digitaliseringen är samtidigt, som jag nämnde inledningsvis, en kraft som påverkar inte bara Försvarsmakten, utan hela vårt samhällsklimat i dagsläget. Här krävs såväl ett tydligt ledarskap för att peka ut den digitala färdriktningen i en föränderlig och osäker omvärld, som ett långsiktigt åtagande från såväl myndigheten som från politiken. Att fatta välinformerade och väl avvägda beslut, med en förståelse för digitaliseringens möjligheter och begränsningar, får sannolikt stor betydelse för Försvarsmaktens möjlighet att lösa sina uppgifter på ett effektivt sätt i en alltmer digitaliserad framtid.

Författaren är överstelöjtnant, flygingenjör, teknologie doktor i informationsteknologi och ledamot av KKrVA. Han tjänstgör som sektionschef i Högkvarteret och är affilierad forskare i försvarssystem vid Försvarshögskolan.

Noter

1. Nato Secret Wide Area Network (NSWAN). Ett gemensamt datornätverk som förser Natos kommandon, medlems- och partnerländer med säker datorkommunikation.
2. Battlefield Information Collection and Exploitation System (BICES). Ett informationssystem som används inom Nato för delgivning av underrättelser och utbyte av information.