



SLUTRAPPORT 2026

Digital regional potential inom **FÖRSVARSMSTÄLLNINGEN** i Västernorrland

bron.

 Sundsvalls
kommun

 Region
Västernorrland

SLUTRAPPORT FÖRSTUDIE:

DIGITAL REGIONAL POTENTIAL INOM FÖRSVARSMÖJLIGHETEN I VÄSTERNORRLAND

Förstudien har genomförts av Bron Innovation

Med medfinansiering av Region Västernorrland och Sundsvalls kommun

2026-01-01 – 2026-09-30

Projektledare: Fredrik Ahlmark

BAKGRUND	4
METOD	5
SAMMANFATTNING	6
BAKGRUND OCH SYFTE	6
HUVUDRESULTAT OCH SLUTSATSER	6
REKOMMENDATIONER OCH VÄGEN FRAMÅT	7
OMVÄRLDSANALYS	8
NATIONELLT OCH INTERNATIONELLT	8
<i>Totalförsvaret byggs upp igen</i>	8
<i>Cybersäkerhet blir en strategisk fråga</i>	8
<i>Nya arbetssätt</i>	9
<i>Gränsöverskridande samverkan i Norden</i>	10
VÄSTERNORRLAND	10
<i>Digital potential</i>	11
JÄMTLAND HÄRJEDALEN	11
VÄRDEKEDJEANALYS	11
REGIONAL UTGÅNGSPUNKT OCH STRATEGISK POSITION	11
<i>Värdekedjans struktur och regional passform</i>	12
<i>Etableringsfokus för stärkt värdekedja</i>	13
SLUTSATS OCH REKOMMENDATION	13
FÖRSLAG PÅ INSATSER FRAMÅT	14
<i>Tvärregional samverkan och ekosystembyggande</i>	14
<i>Kompetenslyft och kunskapsöverföring</i>	14
<i>Leverantörsutveckling och marknadsetablering</i>	14
<i>Kvalitetssäkring, säkerhet och certifiering</i>	15
<i>Fördjupning, tvärregionalt samarbete med internationellt perspektiv</i>	15
FÖRSTUDIENS GENOMFÖRANDE	17
INTERVJUER	17
<i>Försvars- och säkerhetsmarknaden som kund</i>	17
<i>Certifieringar och digital resiliens</i>	18
<i>Upphandling med långa ledtider</i>	19
<i>Behov av regionalt stöd och möjlighet att ingå i konsortium</i>	20
WORKSHOPS	21
<i>Cybersäkerhet</i>	21
<i>Resultat cybersäkerhet</i>	22
<i>Upphandling</i>	22
<i>Resultat upphandling</i>	22
SPRIDNINGSAKTIVITETER	24
<i>Konferens – För säkerhets skull</i>	24
<i>Konferens – Tech i försvarsindustrin</i>	24
REDOVISNING FÖRSTUDIENS CENTRALA FRÅGESTÄLLNINGAR	25

REDOVISNING HÅLLBARHETSPERSPEKTIVEN	27
MILJÖ.....	27
JÄMSTÄLLDHET	27
MÅNGFALD.....	28
BILAGA.....	29
INTERVJUFRÅGOR	29

BAKGRUND

Det säkerhetspolitiska läget i Europa och dess närområde är i dag det allvarligaste sedan andra världskrigets slut. Den fullskaliga ryska invasionen av Ukraina, eskaleringen och säkerhetskrisen i Mellanöstern samt Sveriges fullvärdiga medlemskap i Nato har fundamentalt ritat om kraven på nationell resiliens och civilt försvar. I den moderna hotbilden är totalförsvaret och Försvarsmakten helt beroende av ett fungerande civilsamhälle, robust digital infrastruktur, säker datakommunikation och kvalificerad spetskompetens inom mjukvara och cybersäkerhet.

I denna omställning har Västernorrland, i samverkan med Jämtland Härjedalen, fått en direkt strategisk nyckelroll i den framväxande Natokorridoren - Trondheim, Östersund och Sundsvall. Samtidigt som regionen har världsledande försvarsindustriella verksamheter och starka civila IT-miljöer, har det tidigare saknats ett samlat, faktabaserat underlag som kartlägger i vilken utsträckning länets små och medelstora IT- och mjukvarubolag har förmåga, intresse och affärsmässiga förutsättningar att etablera sig som leverantörer inom försvars- och säkerhetssektorn.

Huvudmålen med förstudien är att:

Kartlägga intresse, potential och hinder: Att undersöka förutsättningarna för regionala företag inom IT-sektorn i Västernorrland att etablera sig som leverantörer till försvars- och säkerhetssektorn.

Stärka värde- och leverantörskedjor: Att beskriva hur dessa kedjor kan förstärkas genom strategiska etableringar i regionen.

Ta fram rekommendationer för en större satsning: Att utarbeta konkreta rekommendationer för framtida insatser för att höja regionens innovationsförmåga och konkurrenskraft inom detta område.

Leverera ett beslutsunderlag: Att ta fram en slutrapport som fungerar som ett förankrat beslutsunderlag för en eventuell större regional satsning som omfattar regionens IT- och mjukvaruföretag, med fokus på cybersäkerhet och affärsmöjligheter inom försvars- och krisberedskapsmarknaden.

Stärka regionens position: Att bidra till att Västernorrland stärker sin ställning inom cybersäkerhet i den pågående försvars- och kris/beredskapsomställningen, med en tydlig koppling till Västernorrlands regionala utvecklingsstrategi (RUS 2030) under målområdet År 2030 är Västernorrland platsen där företag och organisationer väljer att växa med prioriteringarna fler nya och växande företag samt utvecklade styrkeområden genom smart specialisering.

Förstudiens målgrupp är länets små och medelstora IT- och mjukvaruföretag med potential att leverera digitala tjänster och lösningar till civila och offentliga aktörer inom försvar, krisberedskap och samhällssäkerhet.

Uppdragets kärna är att systematiskt utvärdera den regionala digitala kapaciteten genom sex centrala frågeställningar som fördjupas och besvaras i rapportens analysdel:

1. Vilket intresse har regionala IT- och digitaliseringsföretag av att utveckla och leverera tjänster och/eller produkter till försvars- och beredskapssektorn, inklusive både civila och militära aktörer?
2. I vilken utsträckning är företagen redan i dag leverantörer till försvars- och beredskapssektorn, och om så inte är fallet, vilka skäl och hinder upplever företagen för att ta steget in på denna marknad?

3. Vilken kunskapsnivå har företagen avseende de krav och förutsättningar som gäller för att bli leverantör, såsom regelverk, säkerhetsklassning, certifieringar, upphandlingsstrukturer och behov av långsiktiga affärsrelationer?
4. Vilka kunskaps- och kompetensbehov identifierar företagen som avgörande för att kunna möta kraven inom försvars- och beredskapssektorn, exempelvis inom områden som informationssäkerhet, cybersäkerhet, regelefterlevnad och affärsprocesser?
5. Vilka typer av stödinsatser bedömer företagen som mest värdefulla för att stärka deras förutsättningar att bli leverantörer, exempelvis i form av kompetensutveckling, rådgivning, samverkan, finansiering, test- och demonstrationsmiljöer eller tillgång till relevanta nätverk och kontaktnät?
6. Vilka delar av försvars- och beredskapssektorns behov upplever företagen som mest relevanta i förhållande till den egna kompetensen och befintliga erbjudanden, och inom vilka områden ser företagen störst potential att bidra?

Metod

Förstudien har genomförts genom en metodik i fyra sammanhängande steg för att säkerställa hög datakvalitet och källtriangulering mellan empiri, expertbedömningar och strategiska analyser:

1. **Omvärlds- och expertanalys:** Kartläggning av det försvarspolitiska landskapet, tekniska hotbilder och legala krav såsom NIS2 och cybersäkerhetslagen. Omfattar expertintervjuer med centrala aktörer såsom Säkerhets- och försvarsföretagen (SOFF), SME-D samt Försvarsmaktens upphandlingsfunktion för att fånga beställarkrav och inträdesbarriärer.
2. **Regionala företagsintervjuer:** Strukturerade djupintervjuer med 17 regionala IT- och mjukvaruföretag för att kartlägga lokala spetskompetenser och identifiera kompetensbehov, utvecklingsområden, certifieringsgrad samt inställning till konsortiesamverkan. Urvalet är strategiskt och inte statistiskt representativt; resultaten ska läsas som indikationer för de intervjuade företagen, inte som en statistiskt representativ bild av länets IT-företag.
3. **Workshops och konferenser:** Omvärldsanalys och företagsintervjuer har validerats genom dialoger där företag samverkat och delat erfarenheter inom områden som identifierats som kritiska (Cybersäkerhet och Offentlig upphandling). Värdefull kunskap har även inhämtats vid två regionala säkerhetskonferenser: "För säkerhets skull" och "Tech i försvarsindustrin".
4. **Värdekedjeanalys och etableringsbedömning:** Analys av hur regionens värde- och leverantörskedjor kan förstärkas genom strategiska etableringar. Genomförd med stöd av extern specialistkonsult.

SAMMANFATTNING

Rapporten sammanfattar resultaten från förstudien Digital regional potential inom försvarsomställningen i Västernorrland genomförd av Bron Innovation med stöd från Region Västernorrland samt Sundsvalls kommun. Förstudien har genomförts i nära dialog med en parallell förstudie i Region Jämtland Härjedalen för att utvärdera gemensamma förutsättningar i Mittsverige.

Bakgrund och syfte

Det säkerhetspolitiska läget i Europa har genom Rysslands invasion av Ukraina, eskaleringen i Mellanöstern och Sveriges fullvärdiga Nato-medlemskap fundamentalt förändrat kraven på nationell säkerhet och motståndskraft. I den moderna hotbilden, präglad av hybridkrigföring och cyberangrepp, är det civila försvaret och näringslivets digitala resiliens helt avgörande för totalförsvarets samlade förmåga. Samtidigt som staten och alliansen genomför historiska anslagsökningar, och försvarsindustrin expanderar i rekordtakt, har det saknats en samlad bild av i vilken utsträckning Västernorrlands IT- och mjukvaruföretag har förmåga, intresse och affärsmässiga förutsättningar att etablera sig som leverantörer till sektorn. Förstudiens syfte har varit att kartlägga denna digitala kapacitet, analysera värdekedjor och etableringsförutsättningar samt leverera ett förankrat beslutsunderlag för en större regional satsning.

Huvudresultat och slutsatser

Högt marknadsintresse: 82 % (14 av 17 bolag) ser en potentiell tillväxtresa. 76 % (13 av 17 bolag) betraktar redan försvars- och säkerhetsmarknaden som en prioriterad målgrupp.

Etablering via underleverantörsled: 53 % (9 av 17 bolag) levererar redan i dag till försvars- eller beredskapssektorn, men i huvudsak som underleverantörer till industriella systemjättar (t.ex. Saab och BAE Systems Hägglunds) eller mot offentlig sektor. Många bolag föredrar uttryckligen att agera som underleverantörer för att hantera marknadens administrativa trösklar.

Hög säkerhetsmedvetenhet trots låg formell certifiering: 76 % (13 av 17 bolag) saknar formell ISO-certifiering, främst på grund av att kostnaden och administrationen upplevs oproportionerlig för mindre organisationer. Samtidigt har flera bolag säkerhetsprövad personal och processer motsvarande säkerhetsskyddsavtal (SUA). Företagen har vanan och förståelsen för sekretess, men saknar den formella certifieringsstämpeln.

Ekonomiska och administrativa inträdesbarriärer: Företagen ser inte långa ledtider (18–36 månader) som ett primärt hinder (71 % hanterar dem väl tack vare vana vid LOU). De dominerande hindren är stela finansiella urvalskriterier (t.ex. omsättningskrav), byråkratiska Moment 22-situationer kring certifieringar.

Konsortier som strategisk hävstång: Hela 82 % (14 av 17 bolag) vill ingå i regionala affärskonsortier för att gemensamt svara på större upphandlingar. Därtill efterfrågar en majoritet av bolagen nätverk, vägledning, matchmaking och finansieringsstöd.

Regional spetskompetens: Västernorrland har starka förutsättningar att bidra till totalförsvaret utifrån den kompetens som finns i regionen. Identifierade områden är t. ex. inom svensk datasuveränitet och 24/7-övervakning (SOC/NOC), AI Edge lösningar såsom autonom övervakning, resiliert kriskommunikation samt kvalificerad systemutveckling.

Värdekedjans logik – ankarbolag och kompletterande roll:

Analysen identifierar möjligheter med ett nischat erbjudande som nod med hög tillgång på IT-kompetens, kompletterat med att vara en viktig logistik- och digital nod i Nato-passagen (Trondheim–Östersund–Västernorrland).

Etableringsarbetet bör fokuseras på att attrahera ankarbolag, där kompetens, logistik och säkra datacenterlösningar utgör primära tillgångar.

Rekommendationer och vägen framåt

Förstudien rekommenderar att resultaten omsätts i ett tvärregionalt genomförandeprojekt som omfattar Mittsverige (Västernorrland och Jämtland Härjedalen) med Bron Innovation som projektägare. Primära finansieringsvägar utgörs av europeiska regionala utvecklingsfonden (ERUF, särskilt insatsområde 1.7) eller Interreg-programmen, med kompletterande regional medfinansiering.

Satsningen föreslås struktureras kring fyra sammanhängande huvudpunkter:

Tvärregional samverkan och ekosystembyggande: Etablera en gemensam arena mellan Västernorrland och Jämtland Härjedalen för att samla näringsliv, akademi och offentliga aktörer, bygga regionala konsortier och koppla upp regionen mot nationella och europeiska nätverk (till exempel ENDR - European Network of Defence-related Region och finska DDE - Digital Defence Ecosystem).

Kompetenslyft och kunskapsöverföring: Genomföra riktade utbildnings- och kompetensinsatser för att öka förståelsen för försvarsmarknadens affärslogik, upphandlingsregelverk (LOU/LUFS) samt säker systemutveckling.

Leverantörsutveckling och marknadsetablering: Stötta regionala små och medelstora företag med matchmaking mot försvarsjättar (t.ex. BAE Systems Hägglunds och Saab), lotsning vid anbudsförfaranden och tillgång till praktiska test- och simuleringsmiljöer.

Kvalitetssäkring, säkerhet och certifiering: Erbjuda processtöd och gap-analyser för att sänka trösklarna inför ISO 27001, säkerhetsskyddsavtal (SUA) och kraven i cybersäkerhetslagen (NIS2/CRA).

En ansökan om ett genomförandeprojekt har tagits fram med utgångspunkt i resultaten från denna förstudie och den parallella förstudien i Jämtland Härjedalen. Ansökan har lämnats in till Tillväxtverket inom ERUF 1.7, med ansökan om medfinansiering från Region Västernorrland och Region Jämtland Härjedalen.

OMVÄRLDSANALYS

Nationellt och internationellt

Totalförsvaret byggs upp igen

Den säkerhetspolitiska kartan i Europa och dess närområde genomgår en historisk omvandling, utlöst av Rysslands storskaliga invasion av Ukraina, eskaleringen i Mellanöstern samt Sveriges och Finlands fullvärdiga inträde i Nato. Dessa händelser har brutit årtionden av nedrustningsdoktrin och förflyttat nationell säkerhet från perifer förvaltning till kärnan av all samhällsplanering.

Den internationella ambitionen har formaliserats genom Natos utgiftsmål (Haag-överenskommelsen), som stipulerar att medlemsländerna fram till 2035 ska avsätta 5 % av BNP till försvar och säkerhetsrelaterad resiliens. Detta delas upp i minst 3,5 % till kärnförsvaret och upp till 1,5 % till bredare säkerhetsinvesteringar såsom civil beredskap, nätverksförsvaret och skydd av samhällsviktig infrastruktur – områden där IT och digital infrastruktur är direkt berättigade utgifter. Enligt Natos lägesrapport har de europeiska allierade ökat sina försvarsutgifter i rekordtakt, där flera nationer väntas nå målen i förtid.

Nationellt har den svenska regeringen i budgetpropositionen för 2026 tillfört ett historiskt anslagslyft. Försvars- och beredskapsanslagen ökar med 26,6 miljarder kronor (+18 % jämfört med 2025), varav cirka 10 miljarder kronor går direkt till det militära försvaret och 4,7 miljarder kronor i ökat materielanslag (1:3-anslaget). Sveriges försvarsutgifter beräknas nå 2,8 % av BNP under 2026, med en beslutad bana mot 3,5 % till 2030. Den civila delen av totalförsvaret rustas parallellt för att säkerställa uthållighet inom energi, telekommunikation, logistik och hälso- och sjukvård vid höjd beredskap eller ytterst krig.

Satsning	Belopp 2026	Källa
Materielanslag (1:3), ökning	4,7 mdr kr (6,7 mdr 2027, 7,5 mdr 2028)	Regeringen.se, sep. 2025
Ny försvarsinnovationsenhet (under FOI)	6 mnkr (10 mnkr fr.o.m. 2027)	Regeringen.se
Förstärkt materielutvecklingsprogram	50 mnkr/år	Regeringen.se
Nytt kontor för försvarsindustriablering	3 mnkr (5 mnkr 2027, 6 mnkr 2028)	Regeringen.se
Forskningsinfrastruktur	30 mnkr (50 mnkr 2027, 75 mnkr 2028)	Regeringen.se

Cybersäkerhet blir en strategisk fråga

I den moderna hotbilden sker hybridkrigföring, desinformation och digitalt sabotage kontinuerligt i gråzonen under tröskeln för väpnat angrepp. Cybersäkerhet har därmed flyttats från att ha varit en isolerad teknisk IT-fråga till att bli en central lednings- och styrningsfråga för både bolagsstyrelser och offentliga beslutsfattare. Globalt värderas marknaden för försvarscybersäkerhet till mellan 20 och 36 miljarder USD år 2026 med en förväntad tvåsiffrig årlig tillväxttakt (CAGR 10,7–11,7 %), driven av molnbaserade multi-domain-operationer och skydd av industriella styrsystem (OT).

Källa	Marknadsvärde 2026	Prognos	CAGR
MarketsandMarkets	20,3 mdUSD	34,5 mdUSD (2031)	11,2 %
Straits Research	29,9 mdUSD	67,5 mdUSD (2034)	10,7 %
Mordor Intelligence	36,0 mdUSD	62,4 mdUSD (2031)	11,7 %

Parallellt implementeras ett paradigmskifte i det europeiska och svenska regelverket:

Cybersäkerhetslagen: Den svenska implementeringen av EU:s NIS2-direktiv trädde i kraft den 15 januari 2026 och omfattar mellan 6 000 och 8 000 organisationer inom 18 utpekade samhällsviktiga sektorer. Lagen ställer tvingande krav på allriskbaserade säkerhetsåtgärder, kontinuitetsplanering, ledarutbildning samt strikta incidentrapporteringsfrister (anmälan inom 24 respektive 72 timmar). Det Nationella cybersäkerhetscentret (NCSC) har konsoliderats under Försvarets radioanstalt (FRA) för att samordna skyddet.

Leverantörskedjekrav (Supply Chain Security): Cybersäkerhetslagen innebär att kraven överförs nedåt i leverantörskedjan. Stora beställare tvingas ställa verifierade säkerhetskrav på samtliga underleverantörer, vilket medför att även mindre IT-konsulter och mjukvarubolag måste möta strikta säkerhetsregimer för att behålla sina affärer.

Cyber Resilience Act (CRA): EU-förordningen som ställer krav på hård- och mjukvaruprodukters inbyggda säkerhet (Security by Design) under hela livscykeln. Rapporteringsskyldigheterna gäller redan under hösten 2026, medan kraven på CE-märkning för produkter med digitala element implementeras fullt ut under 2027.

Nya arbetssätt

Det traditionella militära upphandlings- och utvecklingssystemet har historiskt präglats av stela regelverk, långsamma specifikationscykler och höga inträdeströsklar anpassade efter stora industrijättar. Som branschorganisationen SME-D framhåller har systemet nu tvingats in i en ekonomi av tid, där det akuta omvärldsläget kräver snabbare teknikleveranser och mer agila anskaffningsprocesser. Försvarmakten och FMV visar en ökad öppenhet för innovationer från den civila tech- och mjukvarusektorn (dual-use).

För att sänka trösklarna har ett flertal nya nationella och europeiska verktyg etablerats:

FMV:s En väg in och Battle Week: FMV lanserade under våren 2026 En väg in som kontaktpunkt för oerfarna leverantörer, samt innovationskonceptet Battle Week i samverkan med FOI och Förvarshögskolan. Här demonstreras civila och militära lösningar mot konkreta operativa utmaningar under fältmässiga förhållanden på max 52 veckor från behov till lösning.

EU:s försvarsindustriprogram (EDIP) och Försvarsfonden (EDF): EDIP-förordningen är i operativ drift med 1,5 miljarder euro (2026–2027) och rymmer en särskild finansieringsström för SME-företag och startups. Samtidigt omfattar EDF:s utlysningar (1 miljard euro årligen) teman som AI-stödd lägesbild, taktiska nätverk och molnsäkerhet under EU Defence Innovation Scheme (EUDIS). Konsortiekrav: minst tre oberoende aktörer från tre EU-länder.

NATO DIANA och Vinnova: Natos accelerator Defence Innovation Accelerator for the North Atlantic (DIANA) erbjuder finansiering, mentorskap och testcenter för civil deep-tech med försvarsrelevans. Vinnova har parallellt genomfört riktade utlysningar för SMF att testa och verifiera civila lösningar mot militära kravstandarder.

Preliminär överenskommelse: I juli nådde Rådet och Europaparlamentet en preliminär politisk överenskommelse om att inrätta programmet Agile and Rapid Defence Innovation (AGILE). Förslaget är ett nytt instrument med en budget på 115 miljoner euro. Syftet med programmet är att stimulera och påskynda EU:s försvarsinnovation bland små- och medelstora företag (SME:s).

Gränsöverskridande samverkan i Norden

Natos utvidgning med Sverige och Finland har förvandlat Norden från ett perifert gränsland till en sammanhängande operations- och logistikyta för alliansen. Genom de nordiska försvarsindustriella nätverken – såsom Digital Defence Ecosystem (DDE) i Finland, NORDSEC i Norge och CenSec i Danmark – etableras gränsöverskridande ekosystem där civila techbolag kopplas samman med försvarsmakterna och de stora systemintegratorerna.

I Europa samlar det EU-finansierade nätverket European Network of Defence-related Regions (ENDR) över 120 regioner som samverkar för tekniköverföring och konsortiebyggande inför EDF-ansökningar. Regioner som Centrala Finland (Jyväskylä) fungerar som direkta förebilder genom att sammanföra akademisk cybersäkerhets- och AI-forskning med försvarssektorns behov. Att etablera kopplingar till dessa nordiska och europeiska nätverk är ett avgörande steg för att bryta regional isolering och ge Mittsveriges företag tillgång till internationella leverantörskedjor.

Västernorrland

Västernorrland har tillsammans med Jämtland Härjedalen en framträdande militärstrategisk ställning genom sitt läge i Natokorridoren som förbinder Atlanten (Trondheim) via Östersund till Västernorrland. Som Ronja Ahlberg (SOFF) framhåller i intervjuunderlaget kan passagen få betydelse som logistikaxel för alliansens världsstödd, vilket ställer direkta krav på regional försörjningsberedskap, skyddade logistikflöden och redundanta digitala stödsystem.

Sveriges försvarsindustriella bas omfattar över 400 bolag men är historiskt starkt koncentrerad till södra och mellersta Sverige (Karlskoga, Linköping, Göteborg, Stockholm). Västernorrland utmärker sig dock som ett av få etablerade industriella ankarområden i norr, där flera världsledande verksamheter nu befinner sig i en historisk expansion:

Örnsköldsvik – BAE Systems Hägglunds och Clavister: BAE Systems Hägglunds är länets industriella flaggskepp med orderböcker på tiotals miljarder kronor för bandgående stridsfordon (CV90 och BvS10) till Sverige och flera Nato-länder. Företaget expanderar mot 3 000 medarbetare och bygger 50 000 kvadratmeter nya produktions- och testytor. Parallellt har cybersäkerhetsföretaget Clavister under 2026 säkrat internationella genombrottsordrar, däribland ett kontrakt värt över 280 MSEK för säker fordonskommunikation till det norska försvaret samt integrering i europeiska ledningssystem. Tillsammans skapar bolagen en massiv efterfrågan på lokal ingenjör- och IT-kapacitet.

Kramfors/Docksta – Dockstavarvet: Det Saab-ägda Dockstavarvet är en global spetsleverantör av militära snabbgående båtsystem (CB90), där verksamheten nu vidareutvecklas mot nästa generations stridsbåtar och autonoma marina ytfarkoster, djupt integrerat i Saabs marina division.

Härnösand – Marin logistikpunkt och beredskapsnav: Härnösand återtar sin historiska roll som marin försvarsort. Kommunen driver en strategisk hamninvestering på närmare 100 MSEK för att möjliggöra snabb övnings- och förflyttningsskapacitet för marina förband mellan Berga och Bottenhavet. Försvarsmakten utbildar årligen värnpliktiga och hemvärnsbataljoner via Västernorrlandsgruppen.

Digital potential

Den tydliga regionala närvaron av fysisk försvars- och fordonstillverkning i Ångermanland kan kompletteras med ett digitalt ben inom försvar och beredskap. Detta faller sig naturligt eftersom digitala lösningar är inbäddade i så gott som samtliga verksamheter som berör försvars- och säkerhetsområdet

Med tyngdpunkt i Medelpad, finns tillgång till en hög andel IT-specialister och en unik koncentration av systemkritiska statliga myndigheter som förlagt sin IT-utveckling och drift hit: Försäkringskassan, Bolagsverket, CSN, Statens tjänstepensionsverk (SPV) och Myndigheten för digital förvaltning (Digg). Även Riksarkivet, med verksamhet i Härnösand och Fränsta, har viktig digital kapacitet i detta perspektiv. Denna bas har skapat ett dynamiskt regionalt tech-ekosystem med såväl etablerade IT-leverantörer som nischade deep-techbolag med stor potential att tillföra viktiga värden i utvecklingen av robusta och resilienta lösningar.

Jämtland Härjedalen

Nato-medlemskapet och det geografiska läget mellan Atlantkusten, Trondheim, Östersund och Bottenhavet etablerar Jämtland Härjedalen som en central logistik- och försvarslänk i Mittnorden. Länet genomgår en omfattande militär återetablering i enlighet med försvarsbeslutet 2020 genom Västernorrlands regemente med Jämtlands fältjägarbatal samt det planerade garnisonsområdet på cirka 110 hektar i Torråsen, Östersund. Tillsammans med järnvägs- och omlastningsknutpunkten i Brunflo skapas ett framskjutet nav för allierad trupp- och materieltransport längs Mittbanan och Inlandsbanan.

Parallellt med den militära uppbyggnaden ökar kraven på cybersäkerhet, robust digital infrastruktur, energiresiliens, civil-militär samverkan och små och medelstora företags integration i totalförsvaret.

De regionala förutsättningarna påminner således i flera delar om varandra, även om den industriella närvaron inte är lika tydlig i Jämtland Härjedalen. Ur förstudiens perspektiv stärks den gemensamma potentialen genom resultatet av den förstudie som genomförts parallellt och där intervjuade bolag precis som i Västernorrland uttrycker ett starkt intresse för att utveckla tjänster och produkter inom detta affärsområde.

VÄRDEKEDJEANALYS

Analysen av försvarsindustrins värdekedja baseras på det externa specialistunderlaget från Sundsvall Advisors (Per Wahlberg) samt genomförda aktörsdialoger och workshops. Syftet är att matcha den nationella försvars- och säkerhetssektorns strukturella behov mot Västernorrlands specifika tillgångar, och identifiera var regionen har bäst förutsättningar att etablera nya verksamheter eller stärka befintliga leverantörsled. Sundsvalls kommun har varit caset som fördjupningarna har utgått från, men slutsatserna bedöms giltiga för hela regionen.

Regional utgångspunkt och strategisk position

Sveriges försvarsindustriella bas är historiskt koncentrerad till ett fåtal kluster i södra och mellersta Sverige (såsom Karlskoga, Linköping och Göteborg). Jämförelsen med dessa miljöer visar att Västernorrland varken har eller bör försöka bygga upp en kopia av ett traditionellt vapenkluster. Regionens trovärdiga och

konkurrenskraftiga erbjudande är i stället kompletterande: en strategisk nod för nordlig försörjningsresiliens, multimodal logistik, livscykelstöd samt säker och suverän digital kapacitet.

Västernorrlands profil vilar på en kombination av:

Militärstrategiskt transportläge: Kuststråket i Sundsvall–Timrå–Härnösand knyter samman E4, E14, Mittbanan mot Trondheim/Atlanten, Ådalsbanan samt flera hamnlägen med logistikkapacitet. Detta etablerar regionen som det östra navet i Nato-passagen.

Energi- och naturresurser: Hög tillgång till förnybar el och industri- och kylvatten, vilket är en avgörande konkurrensfaktor för energikrävande digital infrastruktur och produktion.

Teknisk kompetensbas: Mittuniversitetet (med 1 429 helårsstudenter inom teknik och 83 ingenjörsexamina under 2025) samt en regional arbetsmarknad med över 5 000 IT-specialister och en nettoppendling till Sundsvall på +3 670 personer.

Befintligt industriellt ankare: Världsledande markfordonstillverkning hos BAE Systems Hägglunds i Örnsköldsvik och marint båtbyggande vid Dockstavavret (Saab), vilket ger industriell legitimitet i länet.

Värdekedjans struktur och regional passform

Försvarssektorns värdekedja kan delas in i sex huvudområden. En systematisk matchning mot länets förutsättningar visar var regionen ska prioritera sina etablerings- och utvecklingsinsatser:

Del av värdekedjan	Regionala tillgångar i Västernorrland	Regional potential och nisch	Kritiska gap och utmaningar	Prioritet
Forskning, utbildning & innovation	Mittuniversitetet (forskning inom AI, sensorer, elektronik); samverkansvilja.	Stark utvecklingspotential inom Edge AI, sensorteknik, krislogistik och cybersäkerhet.	Behov av fler säkerhetsklassade forskningsmiljöer och långsiktig finansiering.	Hög
Ingenjör- & konsulttjänster	Stor koncentration av systemutvecklare, molnarkitekter och IT-konsulter.	Skalbar kompetensnod för systemintegration, säker kodning och underleveranser.	Begränsad erfarenhet av militära standarder och formaliserade SUA-processer bland SME.	Hög
Robust datainfrastruktur & molntjänster	Hög tillgång till el, kyla, vatten samt regional datacenterkompetens.	Suveräna molntjänster, säker databehandling och drift under svensk lagstiftning.	Höga krav på nätkapacitet, fysiskt skydd och verifierad redundans; utländskt ägande.	Hög (villkorad)
Logistik, underhåll & livscykelstöd	E4/E14, Mittbanan, Ådalsbanan, Tunadalshamnen samt Sundsvall Logistikpark.	Beredskapslager, reservdelsförsörjning, teknisk service och underhåll för totalförsvaret.	Logistikparkens nyttjandegrad och volymer måste verifieras; skyddsklassade lager.	Hög
Komponent- & delsystemproduktion	Etablerad industritradition, verkstadskompetens och tillgång till industrimark.	Nischad tillverkning av komponenter, kapslingar och mekanik med försvarsinriktning.	Kräver riktade industrisatsningar, tillståndsprocesser och certifieringsanpassning.	Medel

Del av värdekedjan	Regionala tillgångar i Västernorrland	Regional potential och nisch	Kritiska gap och utmaningar	Prioritet
Systemintegration & slutmontering	Industriell mark och närhet till etablerade fordonstillverkare i norr.	Kompletterande montering och integration vid större expansioner.	Mycket hög kapitalintensitet, långa ledtider och stark nationell konkurrens.	Selektiv

Etableringsfokus för stärkt värdekedja

Kartläggningen visar att Västernorrlands etableringsarbete inte primärt bör fokusera på enskilda marktytor eller fysiska tomter, utan på att attrahera ankaretableringar som kan fungera som motorer i den regionala värdekedjan. Regionen förfogar visserligen över betydande kapaciteter – från elintensiv industrimark till smarta transportknutpunkter – men fysisk infrastruktur bygger inte i sig ett försvarsindustriellt ekosystem. Lika angeläget är att ha fokus på industriell funktion och affärslogik.

Varför ankaretableringar är avgörande Försvars- och säkerhetsmarknaden präglas av höga inträdeströsklar, slutna nätverk och rigorösa säkerhetskrav som gör det svårt för enskilda små och medelstora IT- och mjukvaruföretag att ta direkta affärer. Detta bekräftas av förstudieintervjuerna med länets IT-bolag:

I denna miljö är etablerade ankarföretag – större systemhus, integratörer och säkerhetsackrediterade teknikhus – helt avgörande. De besitter befintliga ramavtal och säkerhetsskyddsavtal (SUA), agerar kommersiell buffert och skapar ett lokalt behov av regional spetskompetens. Samtidigt motiverar de investeringar i säkerhetsklassade miljöer och ger lokala konsultbolag draghjälp att utveckla egna försvarsnära produkter och delsystem.

Den regionala passformen och den strategiska positionen har prövats och verifierats med ett antal aktörer nationellt. De delar analysen kring regionens förutsättningar, och i några fall har ett nytt konkret intresse kunna konstateras. Detta bör fångas upp i det regionala etableringsarbetet framöver.

Slutsats och rekommendation

Förstudien visar entydigt att Västernorrland har starka förutsättningar inom den expanderande försvars- och beredskapssektorn, särskilt inom svensk datasuveränitet, cybersäkerhet, industriell mjukvaruarkitektur, sensorer (AI Edge) och logistik. Den avgörande insikten från intervjuer och analyser är att regionens främsta tröskel inte handlar om bristande teknisk kompetens. Hindren är i stället strukturella och affärsmässiga: begränsad kännedom om försvarssektorns slutna affärslogik, tunga administrativa certifieringsprocesser, stela upphandlingskrav samt behov av samverkansstrukturer. Slutsatserna överensstämmer med resultatet av den genomförda förstudien i Jämtland Härjedalen.

Förstudien visar vidare på ett tydligt intresse för detta område som ett nytt innovations- och affärsområde. Genom samverkan mellan Västernorrland och Jämtland Härjedalen finns ett tillräckligt stort antal företag för att forma en kritisk massa, samtidigt som regionernas olika profiler kompletterar varandra.

Värdekedjeanalysen och dialogerna med näringslivet understryker att försvarsomställningen i Västernorrland inte kan bygga enbart på att organisera befintliga konsultresurser. Regionen behöver aktivt arbeta för att attrahera strategiska ankaretableringar – systembolag, försvarsintegratörer och specialiserade industri- eller infrastrukturaktörer – som kan etablera fysiska eller operativa noder i länet.

Ett ankarbolag fungerar som en hävstång: det drar med sig långsiktiga kontrakt, kräver certifierade underleverantörer och skapar stabila volymer som gör att lokala små och medelstora företag vågar investera i sin verksamhet, certifieringar, egen produktutveckling. Etableringsarbetet ska fokuseras kring regionens strategiska fördelar, logistik, tillgång på säker datainfrastruktur samt en kompetensbank inom IT.

Med dessa utgångspunkter genomförde förstudien en workshop, med syfte att identifiera och konkretisera innehåll för ett framtida genomförandeprojekt. Workshopen genomfördes av projektteamet förstärkt med den externa konsult projektet anlitat. Arbetet har stämts av med ytterligare aktörer samt med styrelsen för Bron Innovation AB.

Förslag på insatser framåt

Baserat på förstudiens resultat föreslås att det kommande tvärregionala genomförandeprojektet i Mittsverige operativt struktureras utifrån följande fyra huvudområden och insatser:

Tvärregional samverkan och ekosystembyggande

Regionala samverkansstrukturer och konsortieprogram: Etablera ett formaliserat konsortieprogram lett av Bron Innovation som neutral facilitator. Tillhandahålla juridiska standardavtal (partneravtal) som reglerar immateriella rättigheter (IPR), affärshemligheter och riskdelning, vilket undanröjer prestigerisker och intern konkurrensoro mellan lokala IT-bolag.

Starkare nationella och internationella nätverk: Ansöka om medlemskap i European Network of Defence-related Regions (ENDR) och koppla regionens IT-sektor till nordiska nätverk såsom finska DDE och norska NORDSEC. Etablera en aktiv bevakningsresurs för utlysningar inom EDF och NATO DIANA.

Kompetenslyft och kunskapsöverföring

Öka kunskapen om försvarsmarknaden och dess spelregler: Genomföra riktade utbildningsmoduler och masterclasses kring totalförsvarets uppbyggnad, FMV:s och Försvarsmaktens inköpsvägar, LOU/LUFS-undantag samt försvarssektorns affärslogik.

Kompetenspakt och säker utveckling: Tillsammans med Mittuniversitetets campus i Sundsvall och Östersund möta behovet av utbildning inom säker systemutveckling (Secure Coding/DevSecOps), krisledarskap och teknisk dokumentation utan att driva osund kompetensflytt (kannibalism) inom det regionala näringslivet.

Leverantörsutveckling och marknadsetablering

Etablera riktade matchmaking-insatser och dörröppnare: Organisera strukturerade mötesplatser, speed-dating och Reverse Pitch-sessioner där inköpare och teknikchefer från BAE Systems Hägglunds, Saab, Clavister och FMV möter validerade regionala techbolag.

Anbudshubb och lotsning: Etablera en regional stödfunktion som hjälper SME med anbudskvalificering, analys av skall-krav samt registrering med korrekta SNI-koder och sökord för direktupphandlingar under tröskelvärden (<700 000 SEK).

Ge tillgång till tillämpade testmiljöer: Skapa praktiska test- och simuleringsmiljöer i samverkan med Länsstyrelsen och kommunerna (krisövningar med simulerade avbrott i el- och fiberinfrastruktur samt cyberangrepp), i dialog med det Civil-Militära FoU-centret i Örnköldsvik samt Mittuniversitetets risk- och krisforskningscentrum (RCR).

Kvalitetssäkring, säkerhet och certifiering

Stärka företagens säkerhetsmognad och sänka certifieringströsklar: Etablera ett regionalt processtöd för att guida SME genom gap-analyser och anpassningar inför ISO 27001, säkerhetsskyddsavtal (SUA) och kraven i den nya cybersäkerhetslagen (NIS2/CRA).

Finansieringsstöd: Utreda och etablera en regional stödmekanism (t.ex. utvecklingscheckar) som kan medfinansiera bolagens externa revisions- och certifieringskostnader för att bryta rådande Moment 22.

Fördjupning, tvärregionalt samarbete med internationellt perspektiv

Omvärldsanalys, djupintervjuer och genomförda workshops visar att Västernorrland delar strukturella utmaningar och strategiska möjligheter med Region Jämtland Härjedalen. De parallella förstudier som bedrivits av Bron Innovation i båda länen bekräftar att en gemensam tvärregional ansats (Mittsverige) skapar nödvändig kritisk massa, motverkar suboptimering och etablerar en slagkraftig nod i den framväxande nordiska Nato-korridoren mellan Trondheim, Östersund och Sundsvall.

Samarbetet vilar på en tydlig och funktionell rollfördelning som kompletterar snarare än konkurrerar:

Västernorrland: Fungerar som transportkorridorens östra logistik- och industrinav med hamnarna i Sundsvall och Härnösand, den tunga försvarsfordonstillverkningen hos BAE Systems Hägglunds i Örnköldsvik och Dockstavarvet (Saab), samt en koncentration av över 5 000 civila IT- och cybersäkerhetsspecialister i Sundsvall och Örnköldsvik.

Jämtland Härjedalen: Utgör det framskjutna militära mottagnings- och fältövningsområdet i anslutning till riksgränsen och Atlantförbindelsen. Med återetableringen av Västernorrlands regemente med Jämtlands fältjägarbatal (I 21) och garnisonsområdet Torråsen (110 ha) i Östersund, knutpunkten i Brunflo samt forskning vid Mittuniversitetet campus Östersund, bildas regionens operativa militära och krislogistiska bas.

Förstudierna i Västernorrland och Jämtland Härjedalen pekar ut fyra prioriterade samverkansområden som direkt motsvarar strukturen för det planerade genomförandeprojektet:

Samordnad anbudskvalificering och upphandlingslotsning: Upphandlingskontoren i både Östersund och Sundsvall vittnar om en utbredd osäkerhet kring hur säkerhetskrav bäst formuleras och bemöts. En gemensam stödfunktion kan coacha bolag i båda länen.

Tvärregionala konsortier: Samverkan mellan nischade aktörer över regiongränserna för att bygga gemensam leveranskapacitet för större upphandlingar.

Kompetensförsörjning och anti-kannibalism: En gemensam kompetenspakt tillsammans med Mittuniversitetets båda campus motverkar intern kannibalism på personal när försvarsindustrin växer.

Internationell uppkoppling mot Norden och EU: Tillsammans når regionerna kritisk massa för att ta plats i nätverk som ENDR och finska DDE samt söka medel från EDF och NATO DIANA samt även inom Interregprogrammen Sverige/Norge och Aurora.

Förstudiens genomförande

Intervjuer

Inom ramen för förstudien har 17 djupintervjuer genomförts med ledande befattningshavare (VD, grundare, affärs- och konsultchefer) hos små och medelstora IT- och mjukvaruföretag i Västernorrland under perioden mars till juni 2026. Urvalet har gjorts strategiskt för att fånga upp bredden i länets digitala ekosystem – från etablerade drift- och konsultbolag med hundratals anställda till snabbväxande deep-tech-startups och nischade cybersäkerhetsspecialister. Geografiskt speglar urvalet länets digitala tyngdpunkter med en koncentration till Sundsvall (12 bolag), Örnsköldsvik (3 bolag) och Härnösand (2 bolag).

Totalt sysselsätter de intervjuade företagen 462 medarbetare, varav 105 är kvinnor (23 %) och 357 män (77 %). Könsfördelningen belyser branschens strukturella jämställdhetsutmaning, men uppvisar samtidigt positiva undantag där enskilda bolag har uppnått en helt jämn könsfördelning (cirka 50 % kvinnor). Intervjuerna summeras enligt nedan.

Försvars- och säkerhetsmarknaden som kund

En central intervjufråga undersökte hur länets IT- och mjukvaruföretag betraktar försvars- och säkerhetsmarknaden i dagsläget – om den utgör en prioriterad kundgrupp, en möjlig tillväxtresa eller om den upplevs för avlägsen.

Resultatet från de 17 företagsintervjuerna visar ett mycket högt intresse för sektorn:

- 76 % (13 av 17 företag) ser försvars- och säkerhetsmarknaden som en prioriterad kund eller målgrupp.
- 82 % (14 av 17 företag) bedömer marknaden som en potentiell tillväxtresa.
- 53 % (9 av 17 företag) uppger att de redan i dagsläget levererar mjukvara, infrastruktur eller specialistkompetens till aktörer inom försvarssektorn eller angränsande samhällsviktig verksamhet.

Gällande affärsstrategi och leverantörsroll föredrar 71 % (12 av 17 företag) att agera som underleverantörer till etablerade systemleverantörer och större industrikoncerner (såsom Saab eller BAE Systems Hägglunds), medan 29 % (5 av 17 företag) primärt föredrar att agera som direktleverantörer till Försvarsmakten eller FMV. Samtliga fem företag med direktleverantörsambition understryker dock att de är öppna för båda alternativen beroende på uppdragets karaktär och samarbetsform.

Strategisk inriktning mot försvarsmarknaden	Antal bolag (av 17)	Andel	Regional drivkraft och kommentar
Prioriterad kund / målgrupp	13	76 %	Drivs av ökat marknadstryck och behov av robust digital teknik.
Möjlig tillväxtresa	14	82 %	Skalning av civila innovationer till totalförsvaret (dual-use).
Levererar till sektorn i dag	9	53 %	Erfarenhet finns främst som underkonsulter eller mot offentlig sektor.

Strategisk inriktning mot försvarsmarknaden	Antal bolag (av 17)	Andel	Regional drivkraft och kommentar
Föredrar underleverantörsroll	12	71 %	Bedöms som en mer realistisk väg in med lägre administrativ tröskel.
Föredrar direktleverantörsroll	5	29 %	Drivs av nischade spetsprodukter, men öppna för partnerskap.

"Första tjacket skulle nog egentligen vara att få vara underleverantör till någon [...] att leverera rakt ut till FMV enligt alla statuter och regler, det är ett hästjobb."

– Grundare, specialistbolag inom sensorteknik och telekrig

Denna bild bekräftas av dialogen med Försvarsmaktens upphandlingsfunktion, där det framhålls att myndigheten styrs strikt av upphandlingslagstiftningen och varken kan eller bör forcera processer för att särbehandla mindre bolag. Samtidigt understryker branschorganisationen SOFF att små och medelstora företag i det rådande säkerhetsläget har gått från att vara ett trevligt inslag till att bli helt avgörande förmågebärare, förutsatt att de lär sig sälja operativ effekt och funktion snarare än enbart teknik.

Certifieringar och digital resiliens

Företagens formella certifieringsstatus uppvisar ett markant glapp i förhållande till deras faktiska säkerhetskultur och operativa förmåga:

- 76 % (13 av 17 företag) saknar i dagsläget en formell ledningssystemscertifiering.
- 24 % (4 av 17 företag) innehar en formell ISO 27001-certifiering (ledningssystem för informationssäkerhet).
- 6 % (1 av 17 företag) innehar ISO 9001 (kvalitetsledning).
- 76 % (13 av 17 företag) har däremot redan säkerhetsklassad personal och/eller lokaler och processer som hanterar säkerhetsskyddsavtal (SUA).

Säkerhets- och certifieringsstatus	Antal bolag (av 17)	Andel	Slutsats från intervjuunderlaget
Ej formellt certifierade	13	76 %	Följer principer men avstår formell certifiering på grund av kostnader.
ISO 27001 (Informationssäkerhet)	4	24 %	Etablerad bas finns hos bolag med koncernrygg eller egen datacenterdrift.
ISO 9001 (Kvalitetsledning)	1	6 %	Låg formell täckning, men kvalitetskrav möts via agila projektmetodiker.
Säkerhetsklassning (Personal / Lokal / SUA)	13	76 %	Mycket hög mognad; 3 av 4 bolag hanterar redan skyddsvärd information.

"Tyvärr så ser jag att det är en stor kostnad att följa en ISO-standard för mindre bolag. Det är ju som sagt bara 15 anställda. Och jag tycker att man bygger hinder om man börjar ställa den typen av krav på en verksamhet."

– VD, IT-tjänstebolag specialiserat på systemutveckling

Intervjuerna visar att regionens företag besitter god kännedom om säkerhetskrav och relevanta standarder. Det primära skälet till den låga andelen formella certifieringar är att processen upplevs som en orimlig ekonomisk och administrativ belastning för små bolag. Flera bolag pekar på ett byråkratiskt moment 22 för att slutföra revisionen för en ISO-certifiering krävs ofta ett pågående skarpt kunduppdrag som ställer kravet, men för att vinna uppdraget kräver beställaren att certifikatet redan är på plats. Att hela 76 % av företagen redan har säkerhetsprövad personal bekräftar dock att regionens IT-sektor är djupt förtrogen med sekretesshantering och skyddsvärd verksamhet.

Upphandling med långa ledtider

Försvars- och säkerhetsmarknaden karakteriseras av långa säljcykler och utdragna upphandlingsprocesser, ofta mellan 18 och 36 månader. Företagens förmåga att hantera dessa tidsramar skiljer sig åt beroende på affärsmodell och kassaflöde:

- 71 % (12 av 17 företag) uppger att långa ledtider inte innebär någon större negativ påverkan på deras befintliga verksamhet.
- 29 % (5 av 17 företag) uppger att de långa ledtiderna utgör en mycket stor och kännbar negativ påverkan.

Att en tydlig majoritet (över 70 %) hanterar ledtiderna väl förklaras av deras vana vid offentlig förvaltning. Eftersom en stor del av regionens konsult- och IT-bolag har ramavtal eller löpande uppdrag mot kommuner, regioner och statliga myndigheter via LOU, har de redan byggt en organisationsstruktur och en finansiell uthållighet som tål långsamma inköpsprocesser.

De 5 av 17 företag (29 %) som ser ledtiderna som ett direkt tillväxthinder består uteslutande av mindre produktbolag och teknikstartups med 2–7 anställda. För dessa aktörer binder en flerårig säljcykel upp nyckelpersoner och debiterbar tid utan intäktsgarantier, vilket innebär en betydande likviditetsrisk.

"Vi har ju jobbat i två år för att komma till det här steget, då har vi inte ens börjat debitera på det... Det är ju enormt kostnadsdrivande. Det är det som är utmaningen."

– Grundare, arkitektur- och kommunikationsbolag

Behov av regionalt stöd och möjlighet att ingå i konsortium

Företagens efterfrågan på stöd från Bron Innovation visar en stark prioritering mot relationsbyggande, gemensamma konsortier, samverkan och affärsmatchning:

- 88 % (15 av 17 företag) efterfrågar nätverk, mötesplatser och erfarenhetsutbyte.
- 82 % (14 av 17 företag) vill uttryckligen ingå i regionala konsortier för att tillsammans med andra bolag svara på större upphandlingar.
- 71 % (12 av 17 företag) efterfrågar vägledning, lotsning och information om vägar in i försvarssektorn.
- 65 % (11 av 17 företag) önskar riktad matchmaking gentemot större försvarsaktörer och myndigheter.
- 65 % (11 av 17 företag) efterfrågar rådgivning kring extern finansiering och innovationsstöd (Vinnova, EDF, NATO DIANA).
- 35 % (6 av 17 företag) ser behov av kompetens- och kunskapshöjande aktiviteter inom specifika regelverk.

Typ av önskad stödsats från Bron Innovation	Antal bolag (av 17)	Andel	Företagens motivering och inriktning
Nätverk och erfarenhetsutbyte	15	88 %	Neutral arena för att dela lärdomar och förstå marknaden.
Konsortium – ingå i gemensamma anbud	14	82 %	Gå samman för att klara höga omsättnings- och volymkrav.
Vägledning och väg in	12	71 %	Lotsning genom säkerhetskrav, upphandlingsportaler och koder.
Matchmaking mot systembolag	11	65 %	Etablera direkta dörröppnare till inköpare hos Saab, BAE och FMV.
Finansieringsstöd och ansökningshjälp	11	65 %	Hjälp att söka kaskadfinansiering och försvarsinnovationsmedel.
Kompetens- och kunskapsinsatser	6	35 %	Riktade insatser kring NIS2, CMMC, maskindirektiv och säker kodning.

Intresset för regionala konsortier (14 av 17 företag, 82 %) är ett av förstudiens mest bärande resultat. Mindre bolag diskvalificeras i dag ofta av stela finansiella urvalskriterier (exempelvis krav på en årsomsättning över 100 MSEK), trots att deras tekniska leverans håller högsta klass. Genom att samla kompletterande specialistbolag – såsom mjukvaruutvecklare, hårdvaru-/sensortillverkare och cybersäkerhetsexperter – kan regionen paketera starka, integrerade leveranser.

Flera företagsledare betonar att en formalisering av samverkan är en förutsättning på en mindre regional marknad där bolagen till vardags konkurrerar om samma uppdrag och personal. För att samverkan ska fungera krävs tydliga partneravtal som reglerar immateriella rättigheter (IPR) och affärshemligheter, samt att Bron Innovation agerar som en neutral och sammanhållande facilitator utan kommersiellt egenintresse.

"Hellre att ett antal medelbolag här i Västernorrland får vinna än att någon global koncern ska ta hem sina grejer och lägga i någon annan stad... Kommer den stora upphandlingen så blir det varje liten konsultbubbla som försöker svara... just det här paraplytänket att det behövs två tre konsultbolag som faktiskt hugger tillsammans."

– VD/Konsultchef, IT-konsultbolag i Sundsvall

Workshops

Genomgående ämnen som identifierats i såväl omvärldsanalysen som i djupintervjuerna med de regionala företagen är offentlig upphandling, cybersäkerhet och nytt gemensamt projekt. Dessa tre områden valdes därför ut som teman för de workshops som genomförts inom ramen för förstudien.

Cybersäkerhet

I workshopen medverkade representanter från följande företag och organisationer: Aidare, Sveaskog, Punkt fyra, PolarPoint, Accenture, Yrkesmästaren, Sewing Solutions, Visionite, Redpill Linpro, Portolio, Pylero, Currics, Sam H. Smith, Orange Cyberdefense, Norit samt Bron Innovation.

Orange Cyberdefense presenterade en omvärldsanalys om cybersäkerhet och cyberhot samt praktiska åtgärder för robust cyberhygien. Företaget Pylero presenterade därefter sin pågående certifieringsresa inom ISO 27001.

Följande frågor diskuterades sedan i grupper:

- **Nuläge:** Var står vi i dag kopplat till cyberhygien, NIS2 och krav från försvarsindustrin? Vad har vi och vad saknar vi?
- **Vad är målet?** Vad kan vi göra för att påbörja eller fortsätta vår cybersäkerhetsresa i dag?
- **Hinder:** Vad hindrar oss från att ta nästa steg eller nå våra mål?
- **Affär och möjlighet:** Hur kan detta bli en affär, inte bara ett krav?
- **Behov av stöd:** Vad skulle krävas för att vi ska ta nästa steg?

Workshopdiskussionerna bekräftade att cybersäkerhet är ett område där många företag ser ett växande behov av kunskap, stöd och samverkan. En återkommande slutsats var att samverkan mellan företag, offentliga aktörer och stödorganisationer är avgörande för att sprida kunskap och sänka trösklarna för mindre företag att påbörja ett mer systematiskt säkerhetsarbete.

Deltagarna lyfte en omfattande utbildnings- och kompetensutmaning inom cybersäkerhet, där behovet sträcker sig från grundläggande cyberhygien till avancerad specialistkompetens. Samtidigt upplevs regelverk och standarder som komplexa och svåra att tolka. Certifieringar som ISO 27001 och nya krav kopplade till cybersäkerhetslagen (NIS2) beskrevs som viktiga men svårnavigerade, särskilt för mindre företag som saknar egna säkerhetsspecialister.

Företagen betonade att de största hindren ofta handlar om tid, resurser och kompetens snarare än direkta kostnader. Många använder externa konsulter för att genomföra säkerhetsarbete, men upplever utmaningar kring långsiktig förvaltning, ansvarsfördelning och intern kompetensuppbyggnad. Det efterfrågades därför mer praktiskt stöd i form av gap-analyser och vägledning.

Avslutningsvis underströks att verklig cybersäkerhet inte kan reduceras till tekniska verktyg och brandväggar. Ledarskap, intern organisationskultur och mänskliga beteenden spelar en avgörande roll för den faktiska säkerhetsnivån.

Resultat cybersäkerhet

Slutsatserna från workshop bekräftar att regionens IT-företag besitter en hög teknisk verkshöjd, men att det råder en markant skillnad mellan att implementera tekniska säkerhetslösningar och att etablera ett formellt ledningssystem för informationssäkerhet. De dominerande behoven som framkommit är:

Systematik före punktinsatser: Företagen behöver stöd i att gå från ad hoc-lösningar till integrerade ledningssystem enligt ISO 27001 och kraven i cybersäkerhetslagen.

Ledning och kultur: Cybersäkerhet måste förankras i styrelser och ledningsgrupper; den mänskliga faktorn och intern säkerhetskultur identifieras som den mest avgörande sårbarheten.

Leverantörskedjans sårbarhet: I takt med att storföretag och myndigheter ställer hårdare krav på sina leverantörer måste regionala SME kunna uppvisa verifierad cyberhygien för att inte uteslutas ur värdekedjorna.

Upphandling

Deltagande företag på workshopen var: Framna, Currics, MB Elektro, Future Fridays, EasyScanning, Bron Innovation samt Gustaf Danielsson, chef på upphandlingskontoret i Östersunds kommun.

Följande frågor diskuterades i grupper:

- Vad har ni för kapacitet i dag?
- Vad behöver du göra för att ställa om?
- Vad behöver offentlig sektor göra?

Workshopdiskussionerna visade att många av de hinder som företag upplever kring offentlig upphandling inte enbart handlar om regelverk utan också om kunskap, dialog och relationer. Under workshopen lyftes vikten av att vara proaktiva, bygga nätverk och etablera kontakt med beställare innan upphandlingar publiceras.

En central insikt var att möjligheten att påverka kravställning och omfattning endast är möjlig innan upphandlingen är publicerad publikt, inte efter att den annonserats. Flera deltagare upplevde det som värdefullt att få ökad förståelse för direktupphandlingar och de möjligheter som finns för mindre företag att delta i affärer under gällande tröskelvärden (<700 000 SEK).

Samtalen visade också att många företag upplever att pris ofta ges för stor betydelse i upphandlingar, samtidigt som beställare inte alltid har tillräcklig kompetens för att formulera relevanta krav inom exempelvis IT och cybersäkerhet. Deltagarna efterfrågade mer dialog mellan leverantörer och offentlig sektor.

Resultat upphandling

Upphandling har upprepat kommit upp både under intervjuer samt omvärldsanalys som ett område som både skapar hinder och möjligheter för regionens företag. Tabellen nedan sammanfattar de främsta hinder som nämnts under intervjuer om upphandling:

Upphandling (hinder)	Beskrivning	Exempel
Administration	Komplexa anbudsprocesser som kräver både tid och personal.	Ett specialistbolag beskriver statliga FMV-upphandlingar som ett hästjobb de saknar resurser att fullfölja.
Stela omsättningskrav	Höga finansiella trösklar (t.ex. årsomsättning) som exkluderar mindre tekniskt överlägsna bolag.	Ett IT-bolag diskvalificerades trots bäst teknik på grund av ett stelt omsättningskrav på 100 miljoner kr.
Certifierings-Moment 22	Krav på tunga certifikat (som ISO 27001) som kräver aktiva kunduppdrag för att slutföras och vice versa.	Ett bolag fick inte göra slutrevisionen för ISO utan ett skarpt uppdrag, vilket kunden krävde certifikatet för att ge.
Långa säkerhetsledtider	Långsamma personprövningar (SUA) som gör att småbolag riskerar att tappa affären innan godkännandet är klart.	Handläggningstiderna för säkerhetsprövningar är så utdragna att mindre leverantörer riskerar att förlora kontrakt under tiden.
Dyra förberedelser i förväg	Krav på att i förväg bygga säkra lokaler och rutiner på egen risk utan kontrakt eller intäktsgarantier.	Ett nischbolag tvingades investera två års obetalt anpassningsarbete i sina lokaler för att nå rätt säkerhetsklass.

Samt en tabell som sammanfattar de främsta möjligheterna som nämnts under intervjuer inom området upphandling:

Upphandling (möjligheter)	Beskrivning	Exempel
Underleverantör	Att gå som underleverantör till försvarsjättar är ett betydligt enklare insteg än direktavtal.	Ett spetsbolag integrerar sin mjukvara direkt i ett större försvarsföretags färdiga system.
Konsortier och samverkan	Mindre bolag går ihop i regionala konsortier för att gemensamt möta tunga krav på omsättning och leveransvolym.	Flera tech/IT-bolag lämnar ett gemensamt anbud för att klara finansiella tröskelkrav.
Köp under tröskelvärden	Direktupphandlingar under tröskelvärden möjliggör snabba affärer utan betungande administration.	Ett nischat bolag blir direktvalt för ett mindre krisberedskapsuppdrag tack vare sin synliga spetskompetens.
Marknadsdialog	Deltagande i tidiga dialoger ger SME-bolag chansen att visa sin spetskompetens innan kraven spikas.	Lokala bolag visar upp modern teknik i workshops för att vägleda offentliga aktörer inför kommande behov.
AI-stöd i anbudsarbetet	AI används som en administrativ hävstång för att effektivisera anbudsskrivande.	SME använder AI-verktyg för att identifiera skall-krav och generera formella svar.

Spridningsaktiviteter

Konferens – För säkerhets skull

Konferensen För säkerhets skull arrangerades på Grönborg i Sundsvall mot bakgrund av det snabbt föränderliga säkerhetspolitiska läget, där ökade cyberhot, hybridkrigföring och geopolitisk instabilitet berör alla delar av samhället. Syftet var att ge chefer, beslutsfattare, styrelsemedlemmar och projektledare inom privat och offentlig sektor: kunskap, strategiska perspektiv och handfasta verktyg för att höja organisationers motståndskraft och beredskap.

Under konferensen medverkade experter med erfarenhet från politik, försvar, cybersäkerhet och verksamhetsutveckling:

Peter Hultqvist (riksdagsledamot, ordförande i försvarsutskottet, tidigare försvarsminister)

redogjorde för de historiska och säkerhetspolitiska skeenden som format det rådande läget och gav en samlad geopolitisk analys av Sveriges roll i Nato.

Mikael Strid (cybersäkerhetsexpert och tidigare IT-chef inom Försvarsmakten) belyste den moderna cyberhotbilden, antagonistiska angreppssätt och cybersäkerhetslagens krav, samt redogjorde för hur organisationer kan arbeta proaktivt med digital motståndskraft.

Rimsky Barlari (säkerhetsstrateg på Kvadrat) presenterade strategiska perspektiv på totalförsvar, verksamhetskontinuitet och de avgörande vägval ledningsgrupper ställs inför.

Konferensen samlade 62 deltagare från såväl näringsliv och akademi som offentlig sektor.

Konferens – Tech i försvarsindustrin

Under konferensen Tech i försvarsindustrin, som arrangerades i Sundsvall och modererades av Lars Persson Skandevall (VD för Bron Innovation), samlades representanter från IT- och techföretag, offentlig förvaltning och nationella aktörer för att diskutera hur regionala bolag kan ta plats i det växande ekosystemet kring totalförsvaret.

Konferensen belyste att det moderna totalförsvaret genomgår en snabb teknikutveckling där många av de mest avgörande lösningarna inte längre utvecklas inom den traditionella försvarsindustrin. Civila teknologier inom IT, AI, cybersäkerhet, industriell automation och logistik får i dag en omedelbar operativ tillämpning (dual-use).

Från produkter till förmågor: Marknaden rör sig från att efterfråga isolerade, färdiga försvarsprodukter till att efterfråga konkreta operativa förmågor och funktioner. Detta skapar öppningar för snabbfotade techbolag, men förutsätter att man krokar arm med etablerade systempartners för att navigera marknadens tunga regelverk.

Digital resiliens och svensk rådighet: Totalförsvarets uthållighet kräver inte enbart mjukvarusäkerhet, utan fullständig svensk och europeisk rådighet över data och kritiska driftsmiljöer. Evroc presenterade lösningar för europeiska suveräna moln, medan ITSL Solutions och Combitech lyfte potentialen i fortifierad och fysiskt skyddad digital infrastruktur i regionen.

Konferensen samlade 45 deltagare med bred representation från både privat och offentlig sektor – såväl regionalt som nationellt.

Redovisning förstudiens centrala frågeställningar

Uppdragets kärna är att systematiskt utvärdera den regionala digitala kapaciteten genom de sex frågeställningar:

Fråga 1: Vilket intresse har regionala IT- och digitaliseringsföretag av att utveckla och leverera tjänster och/eller produkter till försvars- och beredskapssektorn, inklusive både civila och militära aktörer?

Sammanfattning: Det regionala intresset är markant och växande, särskilt inom cybersäkerhet, säker datainfrastruktur, Edge AI och krislogistik. Företagen ser sektorn som en naturlig marknad, men medan deep-techbolag har en hög tillväxtambition väljer breda konsultföretag att hålla en medveten portföljbalans för att inte bli ensidigt beroende av försvarskonjunkturen.

Analys: Undersökningen visar att 76 % (13 av 17 företag) ser sektorn som en prioriterad målgrupp och 82 % (14 av 17 företag) ser en potentiell tillväxtresa. Drivkrafterna förstärks av det geopolitiska omvärldsläget och ökade anslag till totalförsvaret. Samtidigt skiljer sig strategierna åt: specialistbolag har som mål att försvarsrelaterade kontrakt ska utgöra 30–40 % av omsättningen, medan större IT-bolag medvetet balanserar sina uppdrag för att bibehålla en bred civil kundbas. Intresset dämpas inte av bristande vilja, utan av att mindre bolag saknar en neutral regional aktör som kan samordna och sänka de administrativa inträdeströsklarna.

Fråga 2: I vilken utsträckning är företagen redan i dag leverantörer till försvars- och beredskapssektorn, och om så inte är fallet, vilka skäl och hinder upplever företagen för att ta steget in på denna marknad?

Sammanfattning: Över hälften av bolagen har pågående leveranser till sektorn, men nästan uteslutande via underleverantörsled till större industrikoncerner eller genom samhällsviktiga civila uppdrag. Huvudhindren för nya affärer är stela omsättningskrav, certifieringskostnader (ISO 27001), långdragna säkerhetsprövningar samt risken att exponeras för fientliga cyberhot.

Analys: Totalt 53 % (9 av 17 bolag) levererar redan i dag lösningar med koppling till försvars- och säkerhetssektorn. Endast ett fåtal har haft direkta myndighetskontrakt. De primära hindren är: finansiella skall-krav där mindre deep-techbolag utesluts av stela omsättningskrav (t.ex. 100 MSEK) trots överlägsen teknik; certifierings-Moment 22 där kunden kräver ISO 27001 för att ge uppdraget men revisionen kräver ett skarpt uppdrag; utdragna ledtider vid säkerhetsprövning (SUA) som innebär stor likviditetsrisk; samt måltavlerisk där specialistbolag undviker att öppet skylta som militära aktörer av oro för cyberangrepp.

Fråga 3: Vilken kunskapsnivå har företagen avseende de krav och förutsättningar som gäller för att bli leverantör, såsom regelverk, säkerhetsklassning, certifieringar, upphandlingsstrukturer och behov av långsiktiga affärsrelationer?

Sammanfattning: Företagens säkerhetsmedvetenhet och operativa erfarenhet av sekretess är generellt mycket god, men förståelsen för militära standarder och dolda försvarsupphandlingar är begränsad. Företagen är vana vid långa ledtider, men hindras av att de saknar de administrativa resurser som formell certifiering förutsätter.

Analys: 76 % (13 av 17 företag) arbetar redan i dag med säkerhetsklassad personal (Säpo-kontroller) och förfogar över låsta lokaler och behörighetsstyrda system motsvarande säkerhetsskyddsavtal (SUA). Därtill

uppgger 71 % (12 av 17 bolag) att långa säljcykler (18–36 månader) inte utgör något hinder, då de har lång erfarenhet av LOU-processer mot offentlig förvaltning och statliga verk.

Det faktiska kunskapsgapet rör militär upphandlingsmetodik: företagen saknar insyn i Försvarsmaktens och FMV:s inköp under tröskelvärden (<700 000 SEK), betydelsen av korrekta SNI-koder samt specifika försvarsstandarder som CMMC och maskinförordningen.

Fråga 4: Vilka kunskaps- och kompetensbehov identifierar företagen som avgörande för att kunna möta kraven inom försvars- och beredskapssektorn, exempelvis inom områden som informationssäkerhet, cybersäkerhet, regelefterlevnad och affärsprocesser?

Sammanfattning: Behoven fokuseras inte mot allmän IT-kunskap, utan mot praktisk implementering av cybersäkerhetslagen (NIS2) och Cyber Resilience Act (CRA), säker systemutveckling (DevSecOps), krisledarskap och industristandarder.

Analys: Fyra prioriterade kompetensområden framträder:

1. Översättning av lagkrav till systemarkitektur
2. Säker systemutveckling (Secure Coding) för traditionella utvecklare
3. Krisledarskap och tillämpade simuleringsövningar (avgrävda fiberkablar, cyberintrång) direkt riktade till företagsledning och styrelser
4. Industriell produktinformation gällande EU:s nya maskinförordning, CE-märkning och Simplified Technical English (STE).

Fråga 5: Vilka typer av stödinsatser bedömer företagen som mest värdefulla för att stärka deras förutsättningar att bli leverantörer, exempelvis i form av kompetensutveckling, rådgivning, samverkan, finansiering, test- och demonstrationsmiljöer eller tillgång till relevanta nätverk och kontaktnät?

Sammanfattning: Företagen prioriterar tillgång till nätverk, neutral koordinering av konsortier, dörröppning mot försvarsjättar samt administrativt stöd för anbud och finansieringsansökningar.

Analys: Efterfrågan av nätverk och erfarenhetsutbyte (88 %), konsortiesamverkan (82 %), vägledning och kontaktnät (71 %), matchmaking (65 %) samt finansieringsstöd och ansökningscoachning (65 %). Kvalitativt efterfrågas att Bron Innovation blir en möjliggörare för processer och samarbeten så att SME kan offerera tillsammans utan oro för lokal konkurrens.

Fråga 6: Vilka delar av försvars- och beredskapssektorns behov upplever företagen som mest relevanta i förhållande till den egna kompetensen och befintliga erbjudanden, och inom vilka områden ser företagen störst potential att bidra?

Sammanfattning: Störst potential finns inom svensk datasuveränitet, 24/7-övervakning (SOC/NOC), decentraliserad AI Edge, feltolerant kriskommunikation, transportlogistik samt senior systemintegration.

Analys: Intervjuerna visar att regionen har spetskompetens inom fem avgörande totalförsvarsområden:

1. Digital suveränitet och säker drift.
2. AI Edge och sensorer
3. Resilienta nätverk
4. Logistik och evakueringsstöd
5. Industriell mjukvaruarkitektur och teknisk dokumentation.

Redovisning hållbarhetsperspektiven

Förstudien har genomgående integrerat de tre dimensionerna av hållbarhet – miljö, jämställdhet och mångfald/inkludering – i såväl metodik och genomförande som i den framtåtriktade analysen för ett kommande genomförandeprojekt. Detta ligger i linje med de särskilda villkoren i Region Västernorrlands beslut (Nyps 20377575) samt den regionala utvecklingsstrategin (RUS 2030).

Miljö

Förstudiens operativa arbete har genomförts resurseffektivt och med minsta möjliga klimatpåverkan genom konsekvent användning av digitala samverkansformer. Merparten av företags- och expertintervjuerna har genomförts via säkra videolänkar, och genomförda workshops har erbjudits i hybridformat för att minimera onödigt resande mellan länets kommuner.

I ett bredare strategiskt perspektiv kopplar förstudien försvarsomställningen till den gröna industriomställningen i Västernorrland. Regionens energi- och klimatstrategi betonar energieffektivitet, robust elförsörjning och cirkulära flöden. Genom att lokalisera robust datainfrastruktur, suveräna datacenter och industriellt underhåll till Västernorrland stärks totalförsvarets resiliens samtidigt som koldioxidavtrycket minimeras i jämförelse med fossilberoende etableringsmiljöer.

Jämställdhet

Förstudien synliggör den strukturella ojämställdhet som historiskt präglat både IT-branschen och försvarssektorn. Kvantitativt visar undersökningen av de 17 deltagande IT- och techföretagen i Västernorrland en samlad personalstyrka på 462 personer, varav 105 är kvinnor (23 %) och 357 män (77 %). På ledande befattningar (VD, ägare och grundare) är mansdominansen ännu mer påtaglig bland de intervjuade nischbolagen.

Samtidigt visar materialet att det finns tydliga regionala förebilder och goda exempel att bygga vidare på:

- Hos etablerade konsultbolag i Sundsvall, såsom Xlent Sundsvall (50 anställda), uppgår andelen kvinnor till 50 % som ett resultat av ett långsiktigt och systematiskt inkluderingsarbete.
- Flera av de mest tongivande rösterna i förstudien – såsom branschorganisationen SOFF:s representant (Ronja Ahlberg), Försvarsmaktens upphandlingsansvariga (Marie Aulin) och grundare inom cybersäkerhet (Polar Point) – är kvinnor som driver på förändring i försvars- och säkerhetssektorn.

Förstudien understryker behovet av ett systematiskt jämställdhetsarbete i det kommande genomförandeprojektet för att aktivt säkra regionens kompetensförsörjning:

- **Breddad rekryteringsbas:** Att exkludera eller missa kvinnliga talanger inom mjukvaruutveckling, IT-arkitektur och cybersäkerhet halverar regionens innovationskraft i ett läge där försvarsjättarna dammsuger marknaden på teknisk personal.
- **Styrning och representation:** Genomförandeprojektet ska tillämpa principer om jämn könsfördelning i projektets styrgrupp, vid tillsättning av paneler och talare vid konferenser samt säkerställa att riktade utbildningsinsatser och traineeprogram aktivt attraherar och lyfter kvinnliga utvecklare och ledare.

Mångfald

I genomförandet av förstudien har ambitionen varit att engagera en bred representation av aktörer för att fånga mångfacetterade perspektiv på försvars- och beredskapsomställningen. Dialoger har förts med såväl mikroföretag med 2–6 anställda som medelstora bolag och internationella koncerner med hundratals medarbetare. Särskild omsorg har lagts vid att synliggöra de mindre företagens unika förutsättningar, innovationskraft och strukturella sårbarheter gentemot stela upphandlingskrav.

En särskild målkonflikt rörande internationell mångfald och nationell säkerhet har identifierats under studiens gång: IT-sektorn är beroende av internationell spetskompetens för systemutveckling och avancerad mjukvarukodning. I vissa säkerhetskänsliga uppdrag kan krav kopplade till medborgarskap, säkerhetsprövning och tillgång till säkerhetsskyddsklassificerade uppgifter begränsa vilka medarbetare som kan delta.

Förstudien visar att lösningen inte är att avstå från mångfald, utan att etablera medvetna arkitektur- och säkerhetsmodeller. Som flera intervjuade bolag framgångsrikt demonstrerar kan system utvecklas i anonyma och isolerade testmiljöer (dual-use-modeller) där internationell specialistkompetens kan bidra till civil-militär innovation utan att komma i konflikt med formella säkerhetsskyddskrav eller hantera skyddsvärda produktionsdata.

BILAGA

Intervjufrågor

Följande strukturerade frågebatteri har legat till grund för djupintervjuerna med de 17 regionala IT- och mjukvaruföretagen i Västernorrland:

Inledande presentation

Berätta kortfattat om era produkter/tjänster. Syftet är att förstå om era produkter/tjänster kan passa in i totalförsvarets behov (försvars- och beredskapsomställning). Tanken är att vi pratar om era möjligheter att vara leverantör inom totalförsvaret, om det är av intresse och vilka hinder vi tillsammans behöver hantera och övervinna.

1. Erbjudande och Dual-Use

- Om vi utgår från era produkter/tjänster, hur skulle de kunna göra nytta i en militär eller krisberedskapskontext?
- Arbetar ni i dag med lösningar som kräver hög dataintegritet, kryptering eller robusthet (t.ex. mot avbrott)?
- Har ni någon teknik som ni tror är i framkant nationellt (t.ex. inom AI, Edge Computing, sensorteknik, plattformslösning eller egen produkt/tjänst)?

2. Marknadsmognad och Ambition

- Intresse: Hur ser ni på försvars- och säkerhetsmarknaden i dag – är det en prioriterad kundgrupp, en möjlig tillväxtresa eller känns det för avlägset? (JA/NEJ)
- Strategi: Skulle ni föredra att vara direktleverantör till Försvarsmakten/FMV, eller ser ni er snarare som underleverantör till stora bolag som BAE Systems Hägglunds eller Saab?
- Erfarenhet: Är ni redan nu eller har ni tidigare levererat till aktörer med höga säkerhetskrav? (JA/NEJ – Berätta mer)
- Upphandlingar: Har ni tidigare deltagit i upphandling mot aktör med höga säkerhetskrav? (JA/NEJ – Berätta mer)

3. Trösklar och Hinder (Det kritiska spåret)

- Certifiering: Vilka certifieringar har ni i dag (t.ex. ISO 9001, ISO 27001, CMMC)? Om inte, vad är det främsta skälet till att ni inte tagit dem?
- Säkerhetsprövning: Har ni kännedom om vad ett säkerhetsskyddsavtal (SUA/SSA) innebär för er personal och era lokaler?
- Ledtider: Försvarsaffärer har ofta långa säljcykler (18–36 månader). Hur påverkar det er vilja att satsa på sektorn?

4. Behov av regionalt stöd och samverkan

- Ekosystem: Hur ser ni på samverkan med andra lokala IT-bolag? Skulle ni kunna tänka er att ingå i ett konsortium för att vinna större upphandlingar?

- Bron Innovation: Vilket konkret stöd skulle ni behöva från oss (t.ex. utbildning i säkerhetsskydd, hjälp med finansieringsansökningar till Vinnova/NATO, eller direkta möten med inköpare)?
- Finansiering: Skulle ni vara intresserade av att söka medel för att anpassa er teknik för försvarsmarknaden (t.ex. kaskadfinansiering)?

5. Reflektioner kring totalförsvarets omställning

Avslutande reflektioner kring den nationella upprustningen och deltagande i förstudiens tematiska workshops och valideringsarenor.