TEKNOLOGISK INSTITUT

Nationalt Forsvars-teknologisk Center

CenSec
CENTER FOR DEFENCE, SPACE & SECURITY

Mod fremtidens forsvarsindustri

Teknologi- og forretningstrends blandt forsvarsvirksomheder i Danmark

Udarbejdet for
Nationalt Forsvarsteknologisk Center
CenSec – Center for Defence, Space & Security

Udgiver
Teknologisk Institut, 2024

Forfattere
Nikolaj Birkkjær Andersen
Arne Hørlück Høeg
Martin Eggert Hansen
Karsten Fröhlich Hougaard

Kontaktperson
Forretningsleder Nikolaj Birkkjær Andersen
nika@teknologisk.dk, +45 7220 1876

ISBN: 978-87-91461-84-2

Foto credits
Omslag: Brian Djurslev. s.4: Rune Dyrholm /Forsvaret. s.7: Mik Dyrby / Forsvaret. s.8: Henning Jespersen-Skree. s.11: Fighter Wing Skrydstrup. s.12: Lise Wenger Rosenwanger /SOLDATEN - de værnepligtiges magasin. s.13: Steffen Fog. s.14-15: Forsvaret. s.19: Tue /Forsvaret. s.21 øverst: Rune Dyrholm /Forsvaret. s.21 nederst: Quadsat. s.22: ODU Denmark. s.23: Fregatten Iver Huitfeldt. s.24: Frederikke Frederiksen /Forsvarskommandoen. s.25: Amonyx. s.26: Mads Rolf Ahrenskjær. s.27: MyDefence. s.28: MyDefence. s.31: Tue Skals. s.32-33: Mads Rolf Ahrenskjær. s.34: Flyvevåbnets Fototjeneste. s.35: SIMA Innovations. s.36: Søren Dreijer og Christian Thøgersen /1.Eskadre. s.37: Brian Djurslev. s.38: Terma. s.40: Trier Industries. s.41: Mik Dyrby. s.42-43: Terma. s.45: Terma. s.46: Terma. s.49: Tue Skals /Forsvaret.

Indhold

> **Krigen i Ukraine og det skiftende geopolitiske landskab har accelereret behovet for innovation og tilpasning i forsvarsindustrien.**

Forord fra Nationalt Forsvarsteknologisk Center

Danmark er et lille land. Ikke mindst i et geopolitisk og forsvarsindustrielt perspektiv. Derfor er det kritisk, at vi i Danmark bruger det, vi er gode til - innovation og forskning – til at skabe de bedst mulige forudsætninger for den danske forsvarsindustri og det danske Forsvar. Nationalt Forsvarsteknologisk Center (NFC) er dedikeret til at fremme innovation og teknologisk fremskridt for at styrke Danmarks forsvarsindustri ved at forbinde forskningsmiljøer og industripartnere.

Rapporten er en vigtig brik i vores arbejde med at forstå og udnytte de teknologiske strømninger, der former fremtiden for Forsvaret. De identificerede trends afspejler de udfordringer og muligheder, der opstår i en tid med hurtig teknologisk udvikling og, desværre, en volatil geopolitik. Rapporten giver os mulighed for at arbejde videre med at omsætte disse trends til at styrke vores teknologiske kapacitet og sikre, at Danmark er i stand til at imødegå fremtidens krav.

For NFC er det afgørende at understøtte den danske forsvarsindustris evne til at tilpasse sig disse trends, hvilket kræver stærke samarbejder mellem forskning, industri og myndigheder. Rapporten fungerer som en katalysator for nye idéer og strategier, der kan hjælpe os med at navigere i et komplekst og konstant foranderligt teknologisk landskab.

Jeg ser frem til, at denne rapport vil inspirere til samarbejder og nye teknologiske gennembrud, der kan forstærke Danmarks position som en førende aktør inden for forsvarsteknologi.

Lars Bo Larsen
Direktør, Nationalt Forsvarsteknologisk Center

Forord fra CenSec

Som direktør for CenSec, Danmarks nationale forsvars-, rum- og sikkerhedsklynge, er det en stor glæde at præsentere denne rapport om trends på forsvarsområdet, som er udarbejdet af Teknologisk Institut.

Denne rapport er særligt vigtig for CenSec og vores medlemmer, da den giver en omfattende kortlægning af de aktuelle og fremtidige trends, der former forsvarsindustrien. Krigen i Ukraine og det skiftende geopolitiske landskab har accelereret behovet for innovation og tilpasning i forsvarsindustrien. Rapporten identificerer fire centrale trends – integration, autonomi, modularitet og forsyningssikkerhed – som alle er afgørende for udviklingen af nye teknologier og forretningsmodeller. Disse trends er ikke kun relevante for forsvarsindustrien, men har også potentiale til at påvirke en bred vifte af industrier og sektorer i Danmark.

CenSec anerkender vigtigheden af at forstå og tilpasse sig disse trends for at sikre, at danske virksomheder forbliver konkurrencedygtige på både europæisk og globalt plan. Rapporten tilbyder ikke kun indsigt i de teknologiske fremskridt, men også i de forretningsmæssige muligheder, der kan opstå som følge af disse udviklinger. Det er vores håb, at rapporten vil inspirere vores medlemmer til at skabe nye produkter og services, der kan styrke Danmarks forsvarsindustri. Jeg ser frem til at se, hvordan denne viden kan omsættes til praksis og bidrage til vækst og innovation i Danmarks forsvarssektor.

Dustin Wilden
Direktør, CenSec

Resumé

Den danske forsvarsindustri er under forandring, drevet af teknologiske fremskridt, geopolitik og nye krav til forretningsmodeller. Disse trends åbner nye muligheder for, hvordan industrien kan operere, samt hvilke produkter og tjenester den kan levere.

Der er primært fire trends, der præger den danske forsvarsindustri. Den første trend er bevægelsen mod flere integrerede systemer, der muliggør interoperabilitet mellem teknologier og platforme. Her er kommando- og kontrolsystemer (C2) omdrejningspunktet, understøttet af en enorm vækst i antallet af sensorer på slagmarken.

Den anden trend er autonomi. Der ses stigende anvendelse af autonome systemer, som droner, på slagmarken og en tilsvarende udvikling af teknologier til at imødegå disse. Derudover ses autonomi i en voksende brug af kunstig intelligens til databehandling samt til automatisering af produktionen.

Den tredje trend er modularitet. Systemer og teknologier designes i stadig højere grad ud fra modulære principper, så de kan tilpasses, opgraderes, serviceres og udskiftes løbende. Det øger fleksibiliteten og levetiden for militært udstyr og understøtter integration af forskellige systemer.

Den fjerde trend er forsyningssikkerhed. Virksomhederne har et stadig større fokus på en stabil og sikker forsyning af komponenter og materialer samt på at opbygge tillid hos slutbrugeren via certificeringer og sikkerhedsgodkendelser.

Foruden de aktuelle fire trends lurer tre fremtidige trends i horisonten for industrien. "Anything as a Service"-tilgangen bringer en serviceorienteret tilgang til forsvarsindustrien, hvor der fokuseres på længerevarende kontrakter og serviceaftaler. Samfundssikkerhed bliver en stadig vigtigere dagsorden med øget fokus på beskyttelse af kritisk infrastruktur mod nye trusler. Kvanteteknologi er den store joker i fremtiden, der rummer potentiale for nybrud inden for sensorer, kommunikation og computere, hvilket kan transformere fremtidens militære operationer.

Den forsvarsteknologiske innovation er stor. I perioden fra 2012 til 2022 er det årlige antal ansøgte patenter relateret til forsvarsteknologi godt tredoblet, med USA i front som den vigtigste spiller. Inden for droneteknologi specifikt er antallet af patentansøgninger mere end 40 gange større i 2022 end i 2012, og her er Kina i front med innovationen. Sverige og Schweiz er de mest innovative europæiske lande på forsvarsområdet, vurderet ud fra deres befolkningsstørrelser. Derudover er tyske Rheinmetall den mest patentsøgende europæiske virksomhed på forsvarsområdet. Ift. befolkningsstørrelse er Danmark det 22. mest patentsøgende land i verden og det 16. mest patentsøgende land i Europa på forsvarsområdet.

Udviklingen i Danmarks forsvarsindustri afspejler den bredere Industri 4.0-bevægelse, der kendes fra andre industrier. Fremtiden for den europæiske forsvarsindustri vil især blive defineret af det transatlantiske samarbejde, den europæiske vilje til at realisere store forsvarsinvesteringer og virksomhedernes evne til at innovere inden for kritiske teknologier.

“ Fra 2012 til 2022 er det årlige antal ansøgte patenter relateret til forsvarsteknologi tre-doblet, med USA i front.

Indledning

Den danske forsvarsindustri er i vækst. Det skyldes især krigen i Ukraine, truslen fra et mere aggressivt Rusland og det gentagne amerikanske krav om en mere ligelig økonomisk byrdedeling i NATO. I takt med at Danmark og Danmarks allierede bruger en større del af BNP på Forsvaret, åbnes en række muligheder for danske virksomheder.

Forsvarsindustrien i Danmark rummer mere end 500 virksomheder, hvoraf nogle er direkte leverandører til det danske forsvar eller til udlandet, og andre er underleverandører til danske eller udenlandske virksomheder.[1] De fleste af virksomhederne har både forsvarsrelaterede kunder og civile kunder, og for virksomhederne i kernen af forsvarsindustrien er EU det største marked (31 % af omsætning) efterfulgt af Danmark (26 %) og USA (23 %). Det er med andre ord en branche med stort internationalt udsyn.

Forsvarsindustrien i Danmark vokser ikke blot, den udvikler sig også som følge af den teknologiske udvikling, forskellige markedsdynamikker, den geopolitiske udvikling og det skiftende behov fra slutbrugerne – navnlig i Ukraine, hvor krigen har accelereret det teknologiske kapløb og synliggjort nye dynamikker på slagmarken. Der er altså en række faktorer, der påvirker den danske forsvarsindustri og giver anledning til nye produkter, funktioner, services og forretningsmodeller.

Denne rapport kortlægger og udfolder aktuelle trends i den danske forsvarsindustri. Igennem dialoger med virksomheder og eksperter har Teknologisk Institut identificeret fire centrale trends, der spiller en vigtig rolle for industrien i 2024: integration, autonomi, modularitet og forsyningssikkerhed. Disse fire beskrives og analyseres igennem rapporten med eksempler fra virksomhederne. Derudover præsenteres kvantitative analyser af europæiske og globale patentsøgninger relateret til forsvarsteknologier, som dermed demonstrerer, hvor i verden den forsvarsteknologiske udvikling sker, hvilke virksomheder der fører an, og hvilke områder udviklingen særligt er centreret om. Endelig præsenterer rapporten tre fremtidige trends, dvs. udviklinger, som virksomhederne er bevidste om, men som endnu ikke for alvor har gjort deres indtog i den danske forsvarsindustri: "Anything as a Service," samfundssikkerhed og kvanteteknologi.

Formålet med denne rapport er at dele viden og skabe synlighed om de teknologiske og forretningsmæssige trends, der former Danmarks forsvarsindustri i dag. Den skal både være til inspiration for læsere, der er godt bekendte

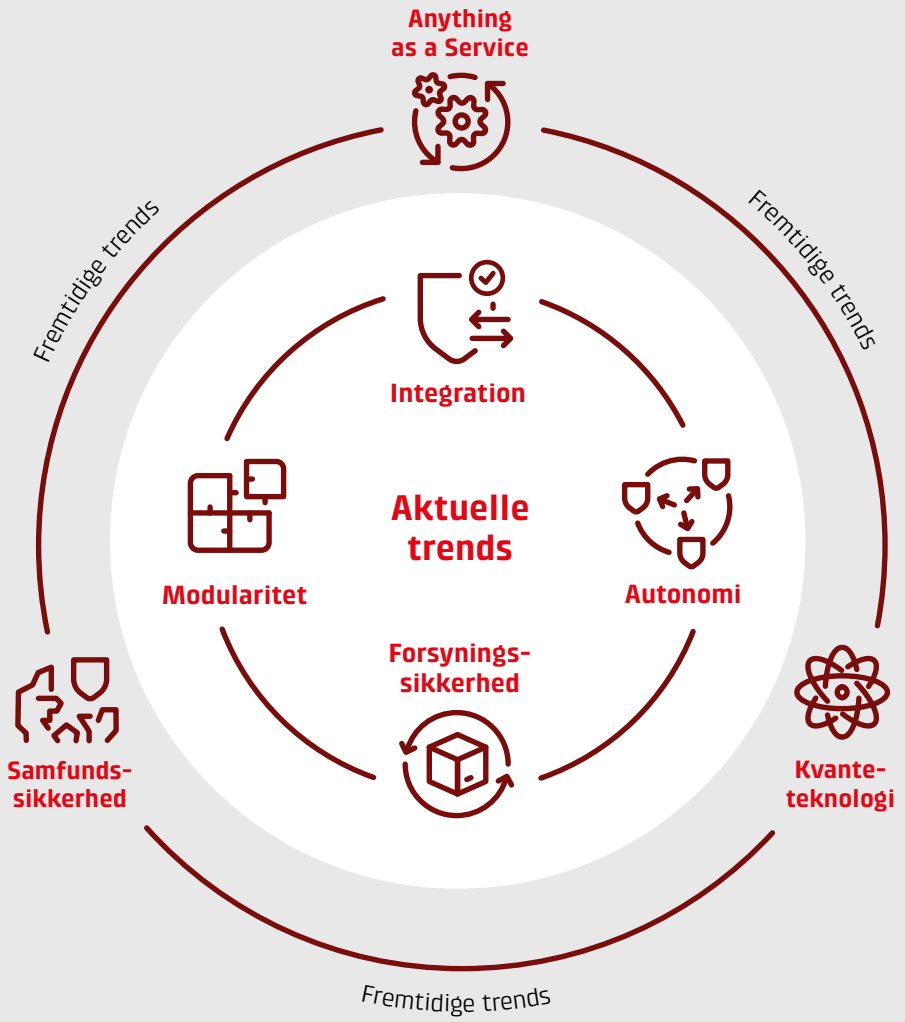
med forsvarsindustrien, og fungere som en introduktion til læsere, der ønsker et større indblik i industrien og dens virksomheder.

Fire aktuelle trends og tre i horisonten

Der er i dag fire temaer, der for alvor sætter dagsordenen for produkt- og forretningsudviklingen i den danske forsvarsindustri (se figur 1): integration, autonomi, modularitet og forsyningssikkerhed. De første tre trends knytter sig primært til teknologi og til de konkrete produkter. Den fjerde, forsyningssikkerhed, handler om virksomhedernes produktion, sikkerhedsforhold og relation til underleverandører. Iblandt de tre fremtidige trends knytter "Anything-as-a-Service" og "samfundssikkerhed" sig til forretningsmodeller og kundesegmenter, mens kvanteteknologi er et teknologiområde med stort potentiale for forsvarsindustrien.

Disse trends er blevet identificeret ud fra virksomhedernes udsagn, der er blevet sammenlignet og analyseret. De identificerede trends bygger altså på industriens egne erfaringer,

Figur 1. Aktuelle og fremtidige trends i Danmarks forsvarsindustri



Teknologiområder i fokus i NATO og NFC

En række teknologiområder er blevet udpeget som strategisk vigtige eller disruptive for Danmark og Danmarks allierede. Et hurtigt blik på to opgørelser tegner et billede af, hvad det er for konkrete teknologier, der nyder fokus fra vigtige organisationer på forsvarsområdet.

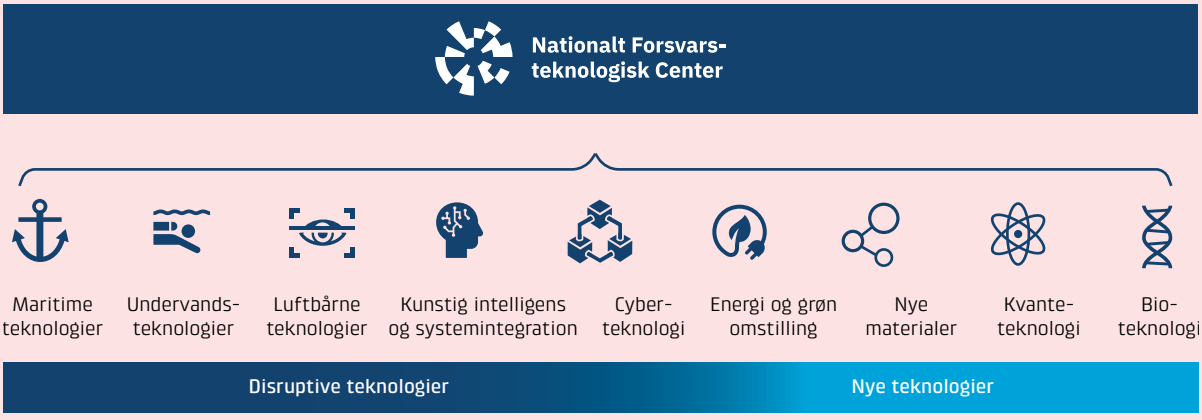
NATO bruger betegnelsen "emerging and disruptive technologies" (EDT) til at beskrive ni strategisk vigtige teknologier, der hver udgør et spor for NATOs innovationsarbejde:[2]

- Kunstig intelligens (AI)
- Autonome systemer
- Kvanteteknologier
- Bioteknologi og "human enhancement"-teknologier
- Rummet
- Hypersoniske systemer
- Nye materialer og produktion
- Energi og fremdrift
- Næste generations kommunikationsnetværk

I Danmark blev Nationalt Forsvarsteknologisk Center (NFC) lanceret i 2023. Her har man siden identificeret ni teknologiske platforme med etablerede vidensmiljøer i Danmark med et "betydeligt uudnyttet potentiale."[3] Her er altså tale om prioritetsområder i krydsfeltet mellem dansk forskning, industri og Forsvarets behov. NFC organiserer de ni platforme på en skala, der går fra teknologier, der allerede disrupter forsvarsområdet, til nye teknologier, hvis potentiale langt fra er realiseret (se figur 2).

Ved at sammenholde de to lister bliver det tydeligt, både hvor den danske forsvarsteknologiske forskning matcher NATOs fokusområder, men også hvilke områder der er særligt vigtige for Danmark og rummer ekstra potentiale i en dansk kontekst.

Figur 2. NFC's ni forsvarsteknologiske platforme



og ikke på fx politiske prioritetsområder eller styrkepositioner. Rapporten her udgør dermed et empirisk bidrag til den offentlige debat om Danmarks forsvarsindustri.

De identificerede trends er ikke unikke for forsvarsindustrien. Men at flere trends går på tværs af forsvarsindustrien og den øvrige danske (og internationale) industri understreger blot, at forsvarsindustrien har god grund til at lade sig inspirere af det øvrige erhvervsliv – og vice versa.

Rapportens tilblivelse og metode

Nærværende rapport er resultatet af et projekt udført af Teknologisk Institut i 2024. Projektet blev delvist finansieret af Uddannelses- og Forskningsstyrelsen via klyngen CenSec og delvist af Nationalt Forsvarsteknologisk Center. Konsulenter fra Teknologisk Institut har stået for indsamling af data, analyse og rapportering.

Projektet bygger på både kvalitative og kvantitative data. På den kvalitative side blev en

række relevante dokumenter fra bl.a. NATO gennemgået. Der blev gennemført seks ekspertinterviews med eksperter fra hhv. Dansk Industri, Dansk Erhverv, Forsvarsakademiet (to personer), National Center for Defence Robotics and Autonomy samt en enkelt uafhængig analytiker.

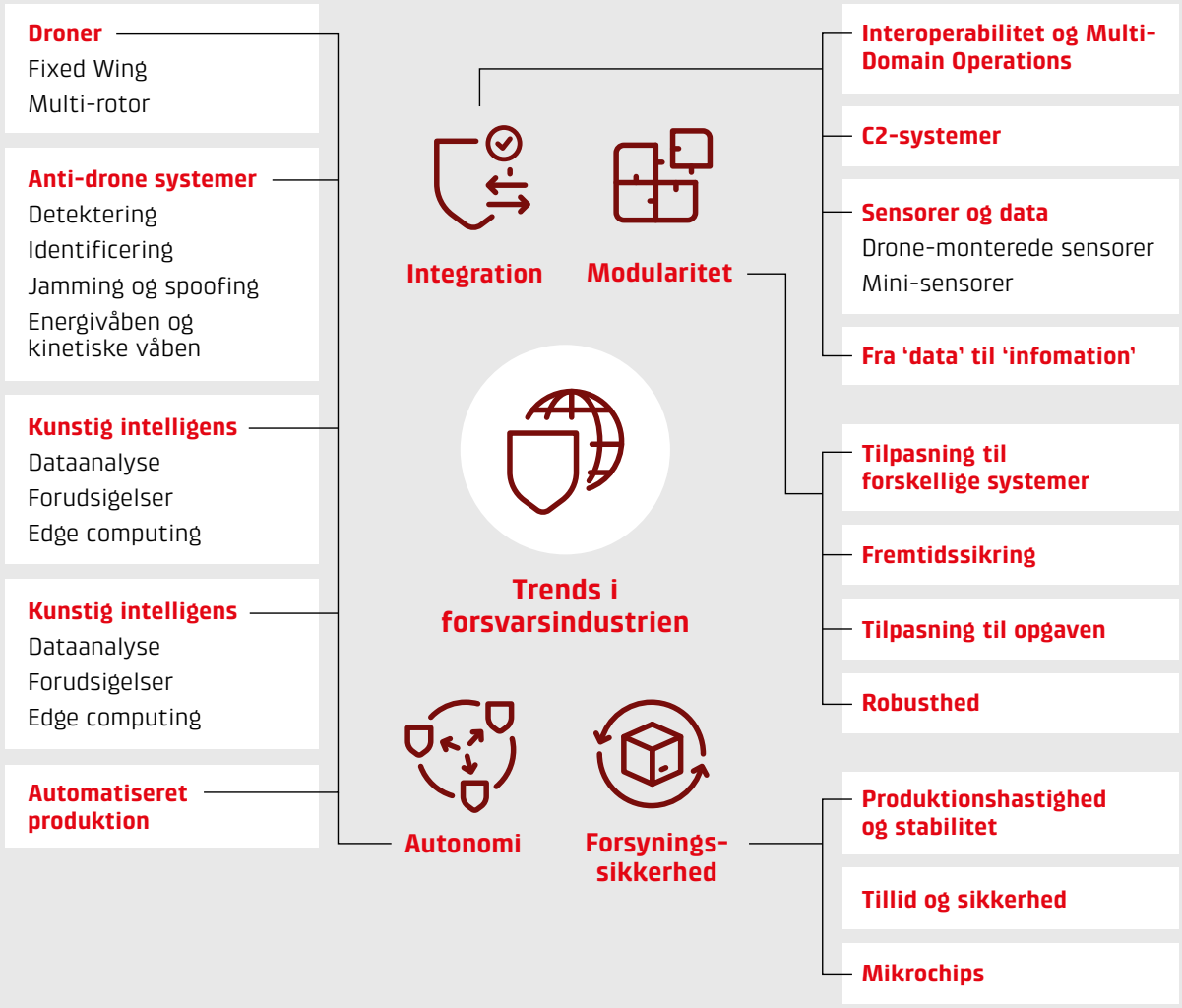
Desuden gennemførtes 16 interviews med virksomheder i Danmark, der er aktive på forsvarsområdet. Blandt de 16 var de største forsvarsvirksomheder Terma, Systematic og Weibel, ligesom en række mindre virksomheder blev interviewet. Tilsammen gav disse interviews et sammenhængende billede af de centrale tendenser i Danmarks forsvarsindustri. Alle interviews var semistrukturerede efter en spørgeramme, der var delt med respondenterne inden interviewet, så de havde mulighed for at forberede sig.

Kvantitativt brugte projektet patentdata som en indikator for innovation. Vi har indhentet data på forsvarsrelaterede patenter og analyseret dem for at kortlægge deres ophav, ansøgervirksomheder, tendenser m.v. Patenter blev identificeret via IPC- og CPC-patentkoder kombineret med søgning på nøgleord i patenternes titler og abstracts. Disse data blev hentet og analyseret via programmet PatSnap og udgør grundlaget for rapportens grafer.

Analysens foreløbige fund blev præsenteret og valideret på en temadag for forsvarsindustrien d. 30. september 2024, der blev afholdt hos Systematic i Aarhus med ca. 35 deltagere. Arrangementet var åbent, og alle virksomheder, der havde deltaget i interviews til projektet, samt alle CenSecs medlemmer blev inviteret. På temadagen blev projektets foreløbige konklusioner diskuteret med virksomhederne, og på baggrund af disse input blev analysen justeret til sin endelige form.

Figur 3. Datakilder i projektet

Figur 4. Oversigt over trends i forsvarsindustrien

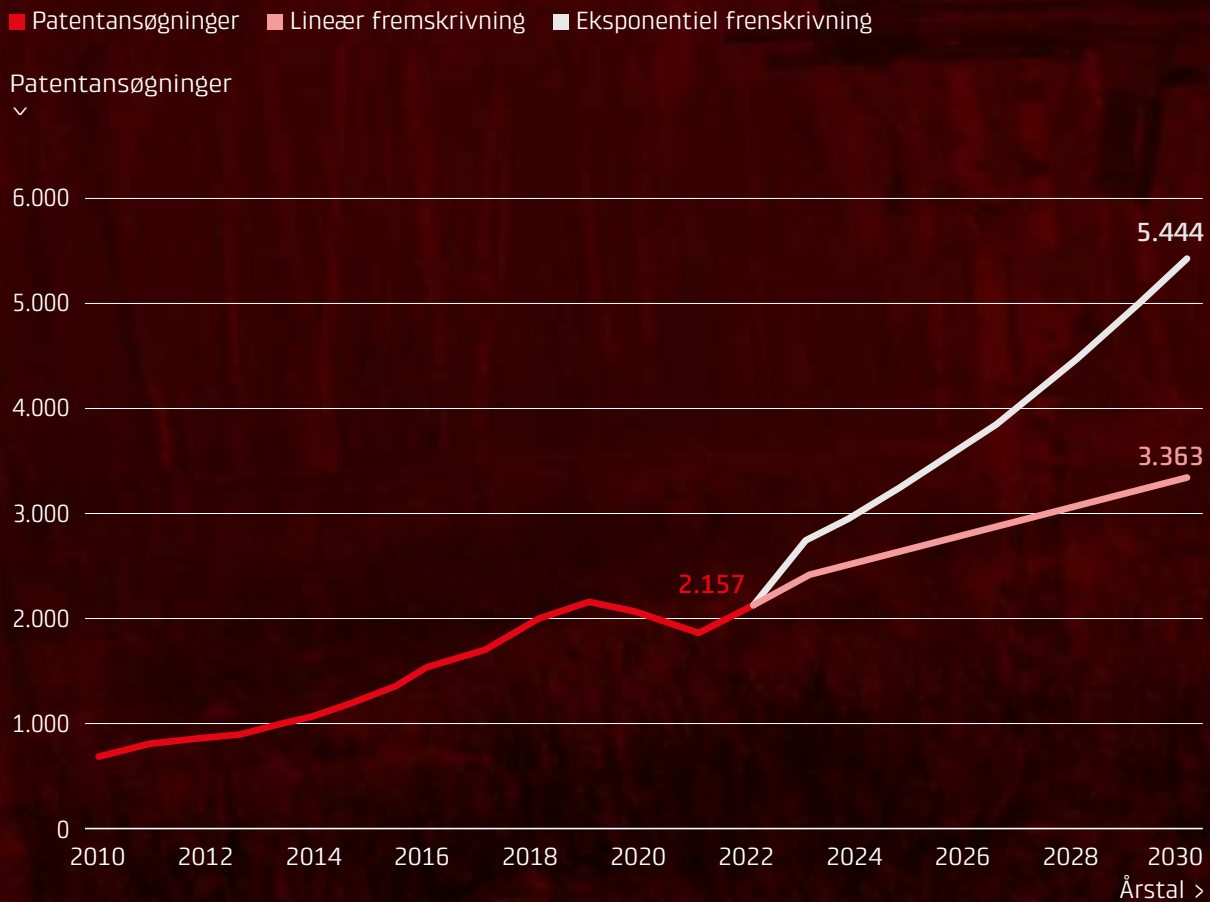


Global forsvarsinnovation

Igennem rapporten præsenteres en kortlægning af den forsvarsteknologiske innovation verden over. Vi har via data om internationale patentansøgninger relateret til forsvarsteknologi identificeret de mest patentsøgende lande og virksomheder i perioden 2010-2022.

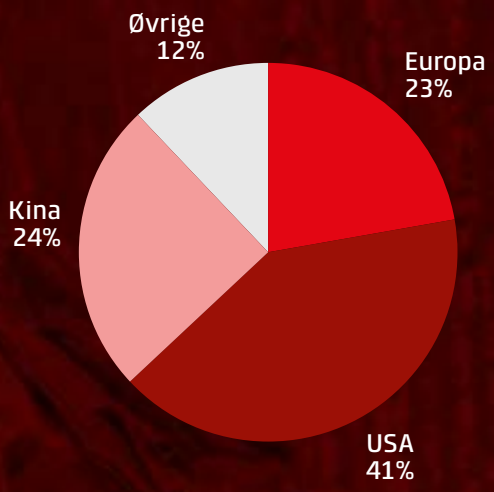
Patentansøgninger er generelt en stærk indikator for innovation, da det er omkostningsfuldt i tid og penge at tage et patent, hvorfor virksomheder generelt kun forsøger at tage patenter på opfindelser, de anser for potentielt værdifulde. Der sker selvfølgelig også meget innovation, der ikke patenteres – især på forsvarsområdet, hvor megen udvikling sker i hemmelige miljøer. Ikke desto mindre giver patenter et indtryk af, hvilke virksomheder der går foran, og hvor i verden udviklingen sker.

Figur 5. Den globale innovation er næsten tredoblet over et årti



Globale patentansøgninger inden for forsvarsteknologi pr. år. Baseret på 19.603 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier. Fremskrivningerne for 2023–2030 er udført af Teknologisk Institut.

Figur 6. USA er i front

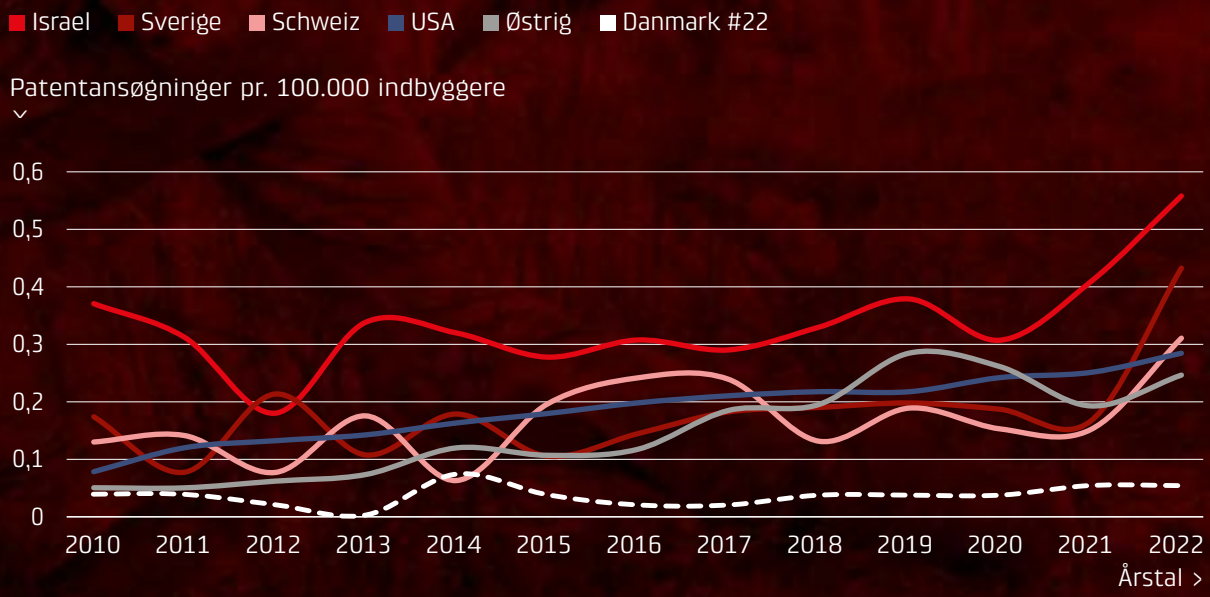


Fordeling af patentansøgninger mellem Europa, USA, Kina og resten af verden. Baseret på 19.603 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier. Europa tæller EU-landene samt Norge, Storbritannien og Schweiz.

Om patentanalyser

Forsvarsrelaterede patenter er afgrænset vha. patentklassifikationerne IPC og CPC samt nøgleordssøgning i patenternes titel, resume og angivne krav. Patenterne strækker sig fra 2010 til 2022 og er opgjort som patentfamilier (dvs. hvis der er udtaget patenter i fem lande på baggrund af én innovation, udgør de én samlet patentfamilie bestående af fem patenter). Patenter skal være udtaget i mindst to lande for at indgå i opgørelsen. Både ansøgte og godkendte patenter er medtaget i opgørelsen.

Figur 7. De mest innovative befolkninger på forsvarsområdet



Baseret på 19.603 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier.

Globalt patentkort

Kortet viser koncentrationen af de 10.000 mest citerede patenter inden for forsvarsteknologi, baseret på ansøgervirksomhedernes adresser. Rød farve indikerer en høj koncentration af ansøgninger.

Trend 1

Integration

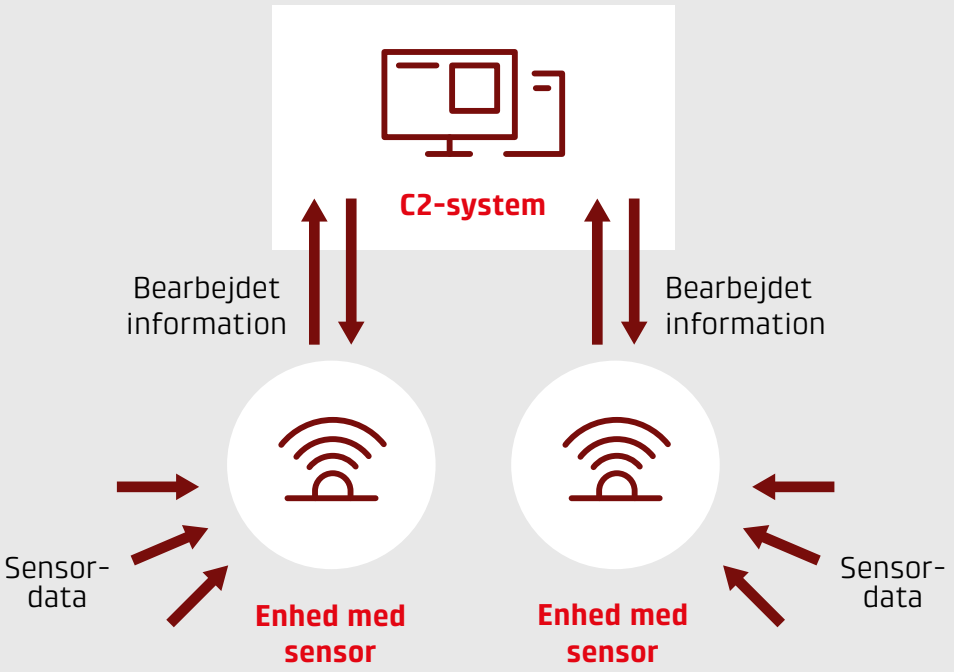
Den første trend i forsvarsindustrien er bevægelsen hen imod mere integration. Danske virksomheder kan ikke nøjes med at fokusere på at udvikle egne produkter og ydelser. Produkterne skal også kunne indgå i helheden af de systemer, som deres kunder bruger. Det betyder, at ethvert produkt skal udvikles med øje for samspillet med andre produkter, software såvel som hardware, hvis det skal være relevant for kunden.

Den første trend er dermed en bevægelse mod mere systemtænkning, hvor platforme og enheder skal kunne tale sammen og gensidigt berige hinanden. Denne integration af fælles systemer tjener flere overordnede formål for et forsvar:

1. Ved at samle data fra mange forskellige kilder, bl.a. forskellige typer sensorer, skabes og deles overblik over slagmarken på tværs af egne enheder.

2. Ved at integrere mange datakilder skabes overblik over egne kapabiliteter, hvilket understøtter ressourcestyring.

Figur 8. Fra sensor til C2



3. Overblik fungerer som beslutningsstøtte på slagmarken, da beslutningstagere får bedre forudsætninger på både taktisk og operativt niveau – potentielt med opdateret data i realtid.

Med trenden "integration" menes altså en større bevidsthed om, at et givent produkt eller en service skal kunne integreres i et større system. Det kan konkret betyde, at data fra en enhed skal kunne integreres i en anden. Det kan også blot betyde interoperabilitet, hvor to systemer kan udveksle information uden at blive slået sammen til et enkelt system. Pointen er den samme: Systemerne indgår i et større hele.[4] I det følgende udfoldes tre elementer af trenden integration: interoperabilitet, sensorer og forholdet mellem data og information.

Interoperabilitet og Multi-Domain Operations

Interoperabilitet betegner i militær sammenhæng evnen til, at udstyr eller grupper kan arbejde eller kommunikere sammen. Princippet er som sådan ikke nyt i militær forstand, da forskellige våbenarter altid har skullet arbejde. Især igennem det 20. og 21. århundrede har samarbejde på tværs af værn – ofte betegnet combined arms eller joint operations – været et nøgletema i militær tænkning, fx i de amerikanske militære doktriner "AirLand Battle" fra 1982 og "AirSea Battle" fra 2010.

Udfordringen med interoperabilitet på tværs af de traditionelle værn er, at hvert værn typisk har sin egen kommandostruktur og sine egne systemer, hvorfor det kræver en ekstraordinær indsats og et tværgående system at dele relevante informationer samt at etablere en klar kommandostruktur på tværs af hierarkierne. Dertil kommer, at værnene kan have forskellige organisationskulturer og interne konflikter, der yderligere besværliggør samarbejdet.

Multi-Domain Operations er NATOs aktuelle formulering af ambitionen om interoperabilitet, der defineres som: "at orkestrere militære aktiviteter på tværs af alle operative domæner og miljøer. Disse aktiviteter er synkroniseret med ikke-militære aktiviteter og gør det muligt for alliancen at skabe de ønskede udfald på rette tid og sted."[5]

NATO har identificeret fem domæner: det maritime, land, luft, rummet og cyber. Interoperabilitet i denne forstand er dermed samarbejde på tværs af disse fem domæner og på tværs af NATOs medlemslande. Derudover adskiller Multi-Domain Operations sig fra traditionelle indsatser på tværs af værn ved at inkludere ikke-militære aktiviteter og eksterne aktører, så som forskning og private virksomheder. Begrebet er altså meget vidtgående ift. de aktører og domæner, der skal kunne samarbejde.

Kommando- og kontrolsystemer

Kommando- og kontrolsystemer (C2-systemer) indfanger kernen af trenden integration. Et C2-system er en integreret softwareplatform, der muliggør effektiv ledelse og styring af militære operationer ved at samle og analysere data fra forskellige kilder. Disse systemer giver beslutningstagere på flere niveauer mulighed for at træffe informerede beslutninger ved

at levere information, potentielt i realtid, om troppebevægelser, fjendens positioner og ressourcestatus. C2-systemer understøtter koordinering og kommunikation mellem forskellige enheder og niveauer i militæret og er designet til at være interoperable med andre systemer.

For leverandører af hele C2-systemer, som Systematic og Terma, stiller interoperabilitet krav til, at deres systemer kan gå på tværs af enheder og ideelt på tværs af værn – eller kan udveksle informationer på tværs af værnenes respektive C2-systemer. C2-systemer skal altså kunne indsamle data, fx om hvor fjendtlige enheder befinder sig, fra en række forskellige platforme og formidle disse informationer til både det operative hovedkvarter og til de relevante taktiske enheder – og ideelt set til alliancepartneres systemer også. Det kræver, at C2-systemerne lever op til en række internationale standarder, så systemerne kan kommunikere sammen.

For leverandører af mere afgrænsede systemer, fx til en enkelt våbenplatform, er det vigtigt, at deres systemer kan oversætte til flere protokoller, så de kan integreres i de større C2-systemer og berige billedet der. De skal kende de mest almindelige C2-systemer og standarder, så deres input kan blive en del af det større system, og brugeren ikke tvinges til at bruge flere parallelle systemer på samme tid. Hvis en virksomhed eksempelvis producerer en sensor, skal data fra sensoren kunne finde vej ind i

Arbit understøtter sikker dataintegration på tværs af sikkerhedsniveauer

Cross Domain-løsninger er et centralt element i NATOs arbejde med Multi-Domain Operations. Begrebet dækker over sikker og kontrolleret udveksling af data og systemer på tværs af sikkerhedsniveauer og domæner. Dette er centralt, når fx C2 eller civile og militære sensordata skal tale sammen, hvilket er centralt for synkronisering i Multi-Domain Operations.

Arbit Cyber Defence Systems udvikler avancerede løsninger til sikker dataoverførsel på tværs af netværk med forskellige klassifikationsniveauer. Deres kerneprodukt, Arbit Data Diode, forhindrer datalækager og beskytter kritiske netværk mod cyberangreb. Og netop dette er afgørende i miljøer, hvor data fra både hemmelige og ikke-hemmelige kilder skal deles uden at kompromittere sikkerheden. Når data bevæger sig fra et system med et højere klassifikationsniveau til et system med et lavere, er det selvsagt essentielt, at der ikke slipper uønskede informationer ud.

Arbits løsninger er bygget med en modulær tilgang, hvilket gør det muligt for dem at tilpasse systemer til datastrømme og sikkerhedskrav.

kundens større system og i sidste ende udgøre en del af det datagrundlag, der præsenteres i C2-systemet.

Sensorer og dataindsamling

En vigtig del af integrationstrenden er den hastige udbredelse af sensorer, der kan levere data til de tværgående C2-systemer. Jo flere sensorer, jo flere datakilder og jo mere præcist et situationsbillede kan potentielt tegnes for beslutningstagere. Sensorer er altså kritiske for kvaliteten af C2-systemerne.

Selvom sensorer og radarer ikke er noget nyt for forsvarsindustrien eller militæret, skaber muligheden for mindre og mere fleksible sensorer nye muligheder, både på og uden for slagmarken – især når sensordata kombineres med algoritmer til databehandling baseret på kunstig intelligens.

På slagmarken er sensorer især relevante, når de monteres på droner, hvor de kan indsamle data om fjendens positioner tæt på frontlinjen, og som foranstaltning mod fjendtlige droner, hvor sensorer kan opfange fjendtlige autonome systemer. Dette uddybes i afsnittet om autonomi.

Sensorer skaber også stor værdi uden for slagmarken. Nordic Radar Solutions udvikler fx radarer til måling og analyse af sprængningsfragmenter, hvilket kan bruges til at måle effektiviteten af skydetræning fra fly eller artillerisystemer. Her kan radarteknologi altså understøtte våbenafprøvning og træning.

Quadsat bruger dronemonterede sensorer til kalibrering af antenner. Deres system kan også udstråle signaler imod antenner, hvilket giver antenneoperatører mulighed for at teste deres systemers modstandsdygtighed imod jamming, dvs. målrettet signalforvrængning. Denne brug af sensorer er muliggjort af, at Quadsats payloads i dag kan laves så små og billige, at de kan monteres på en drone.

Endelig kan sensorer bruges til klassiske logistiske opgaver, såsom at måle beholdninger af ammunition og andet vigtigt materiel, eller til styring af automatisering af lagre. Når denne målefunktion kombineres med kunstig intelligens, giver det mulighed for løbende måling af lagerbeholdning og automatiseret bestilling af forsyninger mv., som man kender fra Smart Warehouse-systemer i den bredere industri.[6]
I en tid med personalemangel kan denne type løsninger være en hjælp for Forsvaret og en mulighed for sensor- og automationsvirksomheder, og potentialet er i dag næsten fuldstændig uforløst i Danmark.

Udviklingen inden for sensorer går mod billigere og mindre sensorer, og det gør det muligt (både praktisk og økonomisk) at montere sensorer på flere systemer, fartøjer og personer. Sammen med de voksende databehandlingskapaciteter giver sensorudviklingen dermed mulighed for at tegne et stadig mere præcist billede af slagmarken på C2-systemerne, hvilket giver beslutningstagere et hidtil uset overblik.

Det er værd at bemærke, at en del sensorteknologi trækker på mange af de samme teknologiske kompetencer som en klassisk dansk industriel styrkeposition: lydindustrien. Det er med andre ord i høj grad den samme type ingeniører, der arbejder med radarer og med høreapparater. Begge dele handler om signalprocessering.[7]

ODU satser på fiberkabler for øget hastighed og sikkerhed

ODU Denmark arbejder med avancerede kabelløsninger, herunder både kobberkabler og fiberkabler, til krævende applikationer i forsvarsindustrien. En af de primære forskelle mellem kobber- og fiberkabler er deres sikkerhedsegenskaber. Fiberkabler er mere sikre end kobberkabler, da de ikke kan jammes eller detekteres, og det gør dem ideelle til brug i militære operationer, hvor kommunikationssikkerhed er afgørende. Kobberkabler udsender elektromagnetiske signaler, der kan opfanges og dermed aflyttes for potentiel følsom information. Desuden er kobberkabler tilsvarende følsomme overfor samme elektromagnetisme, hvilket giver mulighed for at jamme eller kompromittere den information, som overføres.

Fiberkabler transmitterer data via lys, hvilket gør det meget vanskeligt for uautoriserede parter at aflytte eller forstyrre signalerne. Det lave transmissionstab i optiske glasfibre gør det muligt at overføre store mængder data over lange strækninger, samtidig med at fiberkablet giver lavere latency (signalforsinkelse). Sidstnævnte er et vigtigt parameter, når der skal reageres hurtigt, fx på en identificeret trussel. Fiberkabling er desuden lettere og mindre pladskrævende, hvilket gør det nemmere at installere og håndtere i forskellige applikationer, fra skibe over fly til landbaseret mobilt udstyr.

Expanded Beam Performance fiberkabler.

Fra data til information

En central udfordring i integration og interoperabilitet er oversættelsen fra data til information. At slagmarken i dag er tæt befolket af sensorer, betyder, at der er adgang til uoverskueligt store mængder data. Det er helt urealistisk at transportere alle de data fra samtlige sensorer til et fælles C2-system – og dernæst forvente, systemet kan sortere de enorme mængder data. Det ville kræve både gigantisk båndbredde til datatransmission (der oftest sker trådløst) og tilsvarende regnekraft i C2-systemets underliggende hardware.

Derfor må de enkelte systemer ofte selv stå for den indledende behandling af data, så det kun er de relevante data, der sendes videre i kategoriseret og organiseret form. Data skal kort sagt forvandles til information, før de kan berige det større system.

Dette stiller store krav til leverandører af enkelte systemer, som fx dronemonterede sensorer. Selvom disse kan sende et live-feed til en håndholdt enhed, og dermed give den enkelte enhed større indsigt i slagmarken, så kan dette live-feed ikke uden videre transmitteres ind i et fælles C2-system. Helt praktisk vil det i dag fungere på den måde, at en drones operatør selv må rapportere til det fælles system, hvis denne ser noget betydningsfuldt på skærmen. Og dermed er det mennesket, der bruger systemet, som står for oversættelsen fra data (et videofeed eller et billede) til information (fx en melding om en potentiel trussel).

Hvis drømmen om det fuldt integrerede C2-systemet skal realiseres, skal denne manuelle proces automatiseres, så de enkelte systemer selv kan analysere deres datafeed, registrere relevante henvendelser, kategorisere og vurdere disse og sende de relevante informationer ind i C2-systemet. Det kræver videre teknologisk udvikling inden for bl.a. edge computing og mønstergenkendelse baseret på kunstig intelligens, som er en del af trenden "autonomi."

Trend 2

Autonomi

Autonomi er den anden forsvarsteknologiske trend. Den beskriver en industribevægelse hen imod selvkørende processer og produkter samt foranstaltninger mod autonome systemer. Med trenden "autonomi" betegner vi altså både autonome systemer og "anti-autonomi".

I det følgende beskrives fire grene af trenden autonomi: udbredelsen af droner på slagmarken, udbredelsen af anti-drone-systemer, autonomi i databehandling via kunstig intelligens og endelig autonomi i produktionen. De fire emner stikker i forskellige retninger, men understreger alle på forskellige måder, hvordan autonomi er på dagsordenen for virksomhederne i forsvarsindustrien.

Det kan forekomme modstridende at betragte både autonomi og integration som trends inden for industrien. Er de ikke netop modsætninger? Men selvom autonomi kan indebære en form for afkobling, hvilket står i kontrast til integration, handler autonomi fundamentalt om selvstyring, og der er intet, der forhindrer et integreret system i at indeholde selvstyrende elementer. Derfor kan autonomi og integration sagtens sameksistere.

Droner og autonome systemer på slagmarken

Brugen af militære droner har været en kendt del af USA's engagement i Mellemøsten og Nordafrika over de seneste årtier, og sporadisk brug af ubemandede flyvende systemer, som balloner, går langt længere tilbage i historien. Men med krigen i Ukraine har droner indtaget en hidtil uset central rolle i krigsførelsen, og de stridende parter innoverer hele tiden på teknologien bag og brugen af droner på slagmarken. Allerede i 2023 blev det estimeret, at Ukra-

Amonyx: Ny vingeteknologi kan bringe fly og droner til nye højder

Amonyx udvikler vingeteknologi til fly og droner, som kan øge effektiviteten og kapaciteten i luftfarten. Deres teknologi "blown lift" fungerer ved at blæse luft over en vinge på en sådan måde, at det genererer mere løft på et givent vingeareal. Dette gør det muligt for fastvingede fly ("fixed wing") at lande og lette med lavere hastighed, hvilket reducerer behovet for landingsbaner. Derudover mindsker teknologien vindmodstanden på vingen under flyvning, hvilket giver en energibesparelse.

Inden for forsvarsindustrien har Amonyx' teknologi et potentiale for både fastvingede fly og droner. For fastvingede fly betyder det, at militære transportfly kan operere fra kortere og mere improviserede landingsbaner, hvilket er afgørende i krisesituationer, hvor fuldt udviklede lufthavne ofte ikke er tilgængelige. Teknologien gør det også muligt for fly at operere længere på den samme mængde brændstof, hvilket reducerer flyets CO_2-udledning og muliggør længere operationer uden hyppige tankninger – en vigtig faktor for langdistance-missioner såsom patruljering og efterretning.

For droner giver blown lift-teknologien flere operationelle fordele. Droner kan svæve stationært i længere tid, selv under udfordrende vejrforhold, hvilket øger deres evne til effektivt at overvåge specifikke områder, såsom grænsepatruljering, maritim overvågning eller fjendtlige bevægelser. Droner med denne teknologi kan desuden operere ved lavere hastigheder og i lavere højde uden at miste effektiviteten, hvilket gør dem sværere at opdage for fjendtlige radarer og missilsystemer. Denne evne til stealth-operationer gør droner med blown lift-teknologi ideelle til missioner, der kræver lav synlighed.

Teknologien øger også dronernes bæreevne og nyttelastkapacitet. Ligesom med fastvingede fly kan droner udstyret med blown lift-teknologien bære tungere sensorudstyr, kommunikationsudstyr, våbensystemer eller forsyninger over længere distancer, hvilket forbedrer missionernes rækkevidde og effektivitet.

ine mistede 10.000 unmanned aerial vehicles (UAV'er) – eller droner – om måneden, hvilket giver en indikation af den omfattende brug.[8]

Dronekrigsførelsens udbredelse er især drevet af, at droner i dag kan produceres mindre og billigere, hvilket gør dem mere lig ammunition, i funktion og pris, end en større platform, der gerne skal overleve en mission.[9] Og selvom større ubemandede systemer stadig spiller en rolle, er de i høj grad blevet fordrevet fra luftrummet over slagmarken af diverse antiluft-systemer. Derimod kan de helt små droner bevæge sig i meget lave højder, der gør dem svære at ramme.

Den udbredte brug af droner er derfor også blevet et tema for danske virksomheder i forsvarsindustrien, da der er klar efterspørgsel på denne type teknologi, og fordi nogle virksomheder har mulighed for at trække på eksisterende kompetencer fra robot- og droneindustrien i Danmark.

De fleste anvendelser af droner på slagmarken falder i en af to kategorier: rekognoscering eller deciderede kamphandlinger. I begge tilfælde påmonteres en drone en payload, som den bærer med sig. Ved rekognoscering vil denne payload bestå af forskellige typer sensorer til at indsamle billeder og data fra slagmarken. Ved kampdroner vil payloadet typisk være et missil eller en bombe, men der er også en bevægelse mod billige droner, der påmonteres en sprængladning, som dronen vil forsøge at detonere så tæt på en fjende som muligt i "kamikaze"-stil.

I Danmarks forsvarsindustri findes både virksomheder, der bygger hele droner, så som SkyWatch og Nordic Wing, og virksomheder, der udelukkende bygger payloads til montering på droner fra andre virksomheder, såsom Quadsat. Fælles er dog, at danske dronevirksomheder primært fokuserer på droner til rekognoscering og andre funktioner end egentlige kamphandlinger.

Dermed arbejder de danske forsvarsrelaterede dronevirksomheder generelt i krydsfeltet mellem innovationen inden for droneteknologi og inden for sensorer, som beskrevet under afsnittet om integration. Disse droner bruges især til at skaffe viden om fjendtlige positioner og aktiviteter, og enhederne anvendes primært på kompagniniveau og af specialstyrker.

En vigtig del af trenden mod flere autonome systemer er muligheden for at afprøve og udvikle dronerne på slagmarken i Ukraine. Flere af de danske dronevirksomheder har haft droner i luften i Ukraine i 2024 og har haft løbende kontakt med personer på jorden, der kan give feedback på dronernes præstation samt nye behov og udfordringer. Dette giver vigtig feedback til produktudviklingen.

Nogle af de centrale temaer inden for den type droner, som producenterne arbejder med, er:

- dronens mulighed for at fungere i områder, hvor der ikke er adgang til GPS-navigation.
- modstandsdygtighed mod jamming og andre typer elektronisk krigsførelse.
- styringsanordningen fra jorden, der typisk er en form for tablet.
- integration af data med C2-systemer.

Anti-drone systemer

Parallelt med trenden mod flere autonome systemer på slagmarken er der opstået en bevægelse mod flere anti-drone-systemer. De to udviklinger går hånd i hånd, da innovation inden for den ene – fx i forhold til jamming – fører til innovation inden for den anden – fx i modstandsdygtighed overfor jamming.

Anti-drone-systemer udfører generelt en eller flere af fire funktioner:

1. Detektering
2. Identificering
3. Jamming og spoofing
4. Direkte bekæmpelse

Detektering

Detektering af droner er en vigtig funktion på nutidens slagmark, såvel som i forbindelse med beskyttelse af kritisk infrastruktur. Detektering involverer brugen af forskellige typer teknologi til at opdage tilstedeværelsen af droner i et givent område. Virksomheder som Weibel anvender doppler-radarer, der kan spore små og hurtigt bevægende objekter, hvilket gør dem ideelle til at detektere droner, der flyver lavt og hurtigt. MyDefence bruger radiofrekvensteknologi til at opfange radiosignaler mellem droner og deres kontrolenheder.

Effektiv detektering i et større område kan kræve et helt netværk af fikserede sensorer,

der kan dække store områder og operere under forskellige miljøforhold. Men dronedetektorer kan også monteres på fartøjer eller personer. Teknologien er vigtig for at identificere potentielle trusler og give operatører mulighed for at reagere hurtigt. Detekteringssystemer kan desuden integreres i eksisterende sikkerhedsnetværk for at forbedre det samlede overblik.

Identificering

Når en drone er blevet detekteret, er næste skridt at identificere den. Identificering indebærer at fastslå dronens type, oprindelse og potentielle formål. Her anvendes kombinationer af radar, visuelle kameraer og signalanalyse til at skelne mellem forskellige dronemodeller, fx via radiofrekvensanalyse, der kan genkende

Soldaten observerer droner ved hjælp af Wingman dronedetektor og deler informationen via Android Tactical Awareness Kit (ATAK).

MyDefence: Fra vejsidebomber til avanceret anti-drone-teknologi

MyDefence blev grundlagt i 2013 med rødder i behovet for at beskytte soldater mod vejsidebomber i Afghanistan. Virksomheden startede med at udvikle teknologi til at detektere disse trusler, men indså potentialet i at anvende deres ekspertise til den voksende udfordring fra droner, der anvendes i både krigsførelse og civile sammenhænge. Over tid har MyDefence udviklet sig til at blive en førende dansk aktør inden for anti-drone-teknologi, med et stærkt fokus på at detektere, identificere og neutralisere fjendtlige droner.

Virksomhedens teknologi kombinerer flere typer sensorer, herunder radiofrekvens, radar og lyd, for at sikre en effektiv beskyttelse mod droneangreb. MyDefence har udviklet åbne API'er, som gør det muligt for deres systemer at samarbejde med eksisterende C2-systemer, hvilket sikrer interoperabilitet og fleksibilitet. Denne tilgang gør det muligt for deres kunder, der spænder fra militære enheder til kritisk infrastruktur og private sikkerhedsfirmaer, at tilpasse deres forsvarssystemer til skiftende trusselsbilleder.

dronemodellers unikke signalmønstre. Dette er vigtigt for at kunne skelne mellem venlige, neutrale og fjendtlige droner, hvilket er afgørende for at træffe informerede beslutninger om eventuelle modforanstaltninger.

Identificeringssystemer kan også indsamle data til efterretningsformål, hvilket bidrager til en bedre forståelse af trusselsbilledet i et givet område. Præcis identificering er afgørende for at minimere falske alarmer og sikre, at de korrekte handlinger tages i forhold til en aktuel trussel. Denne proces er også et kritisk element i effektive luftforsvarssystemer, der kræver både sofistikeret teknologi og hurtig reaktionsevne.

Jamming og spoofing

Jamming og spoofing er defensive tekniker, der bruges til at forstyrre en drones kommunikation med dens operatør, hvilket kan forhindre dronen i at udføre sin mission. Ved at sende signaler på samme frekvens som dronens kontrolsystem kan jammeren blokere kommunikationen, hvilket kan få dronen til at lande eller returnere til sin startposition. Spoofing går skridtet videre og forsøger at overtage kontrollen med dronen ved at sende målrettede signaler til dens kommunikationsanlæg. Begge dele er særligt nyttigt i situationer, hvor droner udgør en trussel mod sikkerheden, såsom i nærheden af lufthavne eller på slagmarken.

Af de to ovennævnte fylder jamming mest på det danske marked. Jamming-systemer, som dem udviklet af MyDefence, er designet til at være bærbare, så de hurtigt kan tages i brug af soldater på slagmarken. Deres effektivitet afhænger af flere faktorer, herunder rækkevidde, signalstyrke og dronens teknologi.

Direkte bekæmpelse

Den sidste type anti-drone-systemer er den mere hårdhændede respons, hvor man forsøger at beskadige eller ødelægge en fjendtlig drone, fx når soldater nedskyder droner med deres konventionelle våben. Der udvikles dog også nye våben, såsom laservåben eller mikrobølgesystemer, der kan ødelægge dronernes elektroniske systemer.

I Danmark udvikler virksomheden Renegade UxS anti-drone droner, der er selvstyrende og kan skelne mellem venlige og fjendtlige droner samt andre objekter, såsom fugle mm. Når enhederne identificerer en fjendtlig drone, flyver de imod den og kolliderer med den, så den beskadiges eller indfanges.

Kunstig intelligens og edge computing

Kunstig Intelligens rummer enormt potentiale for forsvarsindustrien og er et emne virksomhederne forholder sig aktivt til. Ligesom i andre industrier anses kunstig intelligens' potentiale for stadig at være relativt uudnyttet i forsvarsindustrien, og virksomheder eksperimenterer aktivt med nye anvendelser af teknologien. Der er dog særligt tre anvendelser af kunstig intelligens, der er relevant for virksomhederne: Dataanalyse, forudsigelser og koblingen til edge computing.

Kunstig intelligens kan for alvor accelerere dataanalyse af store og komplekse datamængder. Her kan maskinlæringsalgoritmer trænes til at genkende bestemte mønstre, og på dette grundlag klassificere fremtidige data automatisk. Weibel bruger fx kunstig intelligens til at analysere data fra radarer, så systemet selv kan genkende de forskellige bevægelsesmønstre fra bl.a. droner og fugle. Dermed kan systemet trænes til kun at reagere på de relevante bevægelser. Samme type teknologi bruges til behandling af data fra dronemonterede sensorer og til identifikation af eksempelvis fjendtlige køretøjer på billederne. Alt sammen processer, der betyder, at man ikke behøver at have et menneskes øje på samtlige datastrømme, men at systemet selv kan sige til, når der er behov.

Forudsigelser er en anden konkret måde at bruge kunstig intelligens på, der bygger oven på mønstergenkendelse i store datamængder. Databaserede forudsigelser er kendt fra software i andre brancher. Her kortlægges mønstre for korrelationer i en række forskellige faktorer, der efterfølgende kan bruges til at give kvalificerede estimater på fremtidige sammenhænge, hvor nogle af faktorerne er kendte. Kunstig intelligens er en enorm ressource i denne type analyse, da den kan overskue og gennemskue mønstre i langt mere omfattende materiale, end hvad der kan klares manuelt.

Endelig er edge computing et vigtigt tema i relation til databehandling og potentielt brugen af kunstig intelligens. I edge computing flyttes selve dataprocesseringen ud til "kanten", dvs. den enhed, der indsamler data, fremfor at alt data skal transmitteres og efterfølgende behandles. Som nævnt i afsnittet om integration er dette et vigtigt element i at begrænse de ellers enorme datastrømme, der løber fra fx en sensor til det større system. Terma arbejder på at gøre deres ubemandede systemer i stand til i endnu højere grad automatisk at bearbejde data til information, før det sendes videre, hvilket begrænser mængden af transmitteret data kraftigt. Processen gør desuden datastrømmen mindre sårbar for at blive opsnappet eller jammet af en fjende.

Systematic bruger kunstig intelligens til at støtte beslutningstagere på kamppladsen

It-virksomheden Systematic leverer i dag kommando- og kontrolsystemer til militære enheder og hovedkvarterer i mere end 50 lande, der muliggør planlægning og udførelse af militære operationer i både kriser, krig og ved naturkatastrofer. Systematic anvender kunstig intelligens til analyse af store mængder data for at identificere mønstre i data, billeder og tekst, der kan afsløre relationer mellem forskellige faktorer og munde ud i beslutningsforslag. Eksplosionen i antallet af sensorinformationer gør det nødvendigt at bruge kunstig intelligens for at kunne overskue de enorme datastrømme og udvælge de relevante informationer, der skal indgå i analysegrundlaget. Ellers er der stor risiko for, at alene mængden af informationer medfører handlingslammelse i stedet for det modsatte.

Systematic arbejder også med at bruge kunstig intelligens i deres C4ISR-software til at forudsige udviklingsmuligheder af situationen på kamppladsen og give forslag, hvordan de militære stabe og enheder kan reagere hurtigt og effektivt. Denne type analyse og forudsigelse af udviklingen på slagmarken har militære stabe foretaget efter bedste evne igennem århundreder, men med kunstig intelligens og digitalisering af kamppladsen kan militære beslutninger baseres på langt mere omfattende datamateriale, end mennesker nogensinde vil kunne overskue.

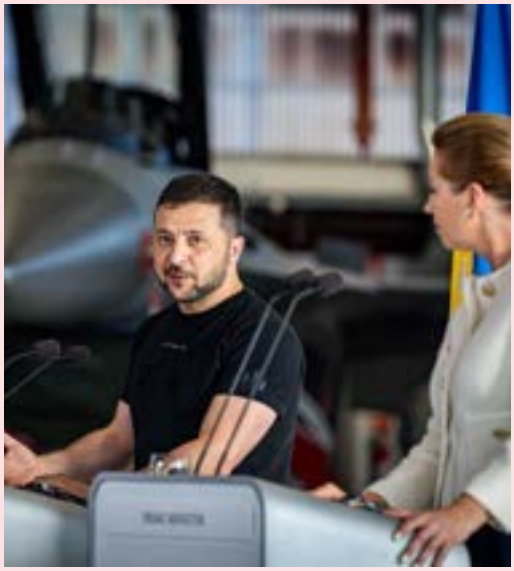
Automatiseret produktion

Endelig ses trenden autonomi i bevægelsen mod mere automatiserede produktioner, der anvender samlebånd, robotarme o.l. Dette tema er især aktuelt givet den udbredte mangel på arbejdskraft samt det relativt høje lønniveau i Danmark. Der er kort sagt stort økonomisk potentiale i automatisering. Hos Trier Industries anvendes robotløsninger drevet af kunstig intelligens til at håndtere komplekse opgaver, hvilket sikrer konsistens og reducerer behovet for manuel indgriben i produktionen. Ligeledes har Multicut integreret en høj grad af automatisering i deres fremstilling af metaldele til forsvarsindustrien. Begge virksomheder demonstrerer, hvordan AI kan optimere kvalitetssikring og omkostningseffektivitet, hvilket er essentielt for at forblive konkurrencedygtig i en global industri.

Potentialet for automatisering er stadig stort – og her har danske virksomheder mulighed for at trække på den omfattende danske ekspertise inden for robotteknologi og automatisering, der kendes fra det danske økosystem for robotteknologi. Når Danmark fx skal i gang med sin egen ammunitionsproduktion, vil det være oplagt at tænke i automatiserede løsninger. Det samme vil gøre sig gældende for en eventuel fremtidig produktion af danske patruljeskibe.

National Center for Defence Robotics and Autonomy

At robotteknologi og automatisering er centrale temaer i den danske forsvarsindustri, ses i oprettelsen af Center for Defence Robotics and Autonomy i november 2024. Centret er etableret af Nationalt Forsvarsteknologisk Center (NFC) og lokaliseret på Syddansk Universitet, hvor det skal være bindeled mellem forsvarsindustrien, universitetsforskning, Danmarks godkendte teknologiske serviceinstitutter (GTS'er, såsom Teknologisk Institut, Force Technology og Alexandra Instituttet), Forsvarsministeriet og Forsvaret. Centret skal trække på den danske styrkeposition inden for robotteknologi og autonomi og har som central opgave at styrke det danske bidrag til krigen i Ukraine, indledningsvis med fokus på droner. Centret skal derfor også arbejde tæt sammen med det danske forsvarskontor i Kiev, EU's Defence

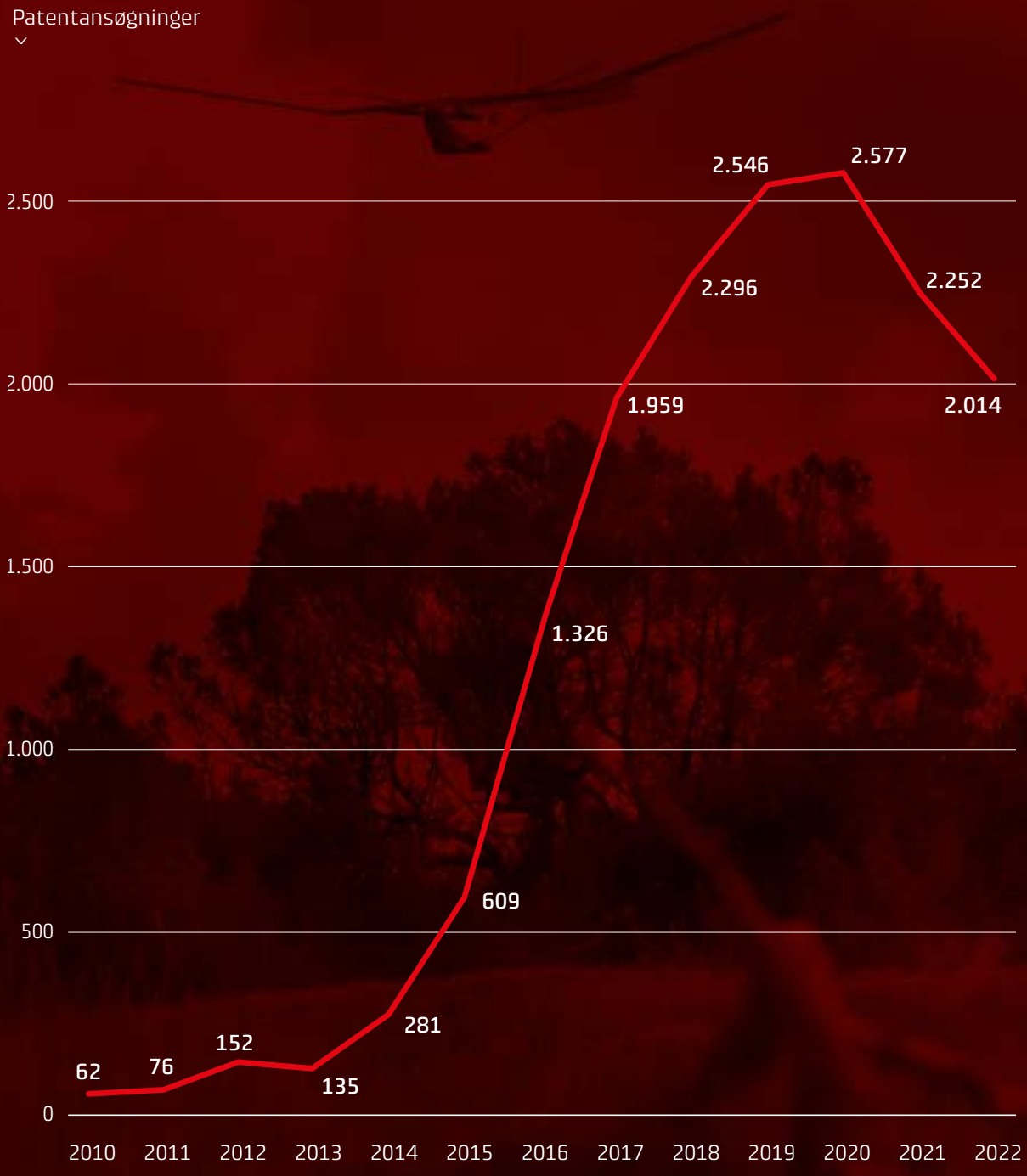


Innovation Office i Kiev samt forsknings- og innovationskontoret i Bruxelles.

Centrets ambition er, at det skal være med til at koordinere det forsvarsteknologiske økosystem, indledningsvis med fokus på droner, så Forsvarets behov, forskningen, kapacitetsudviklingen og skaleringen af produktionen i virksomhederne bindes

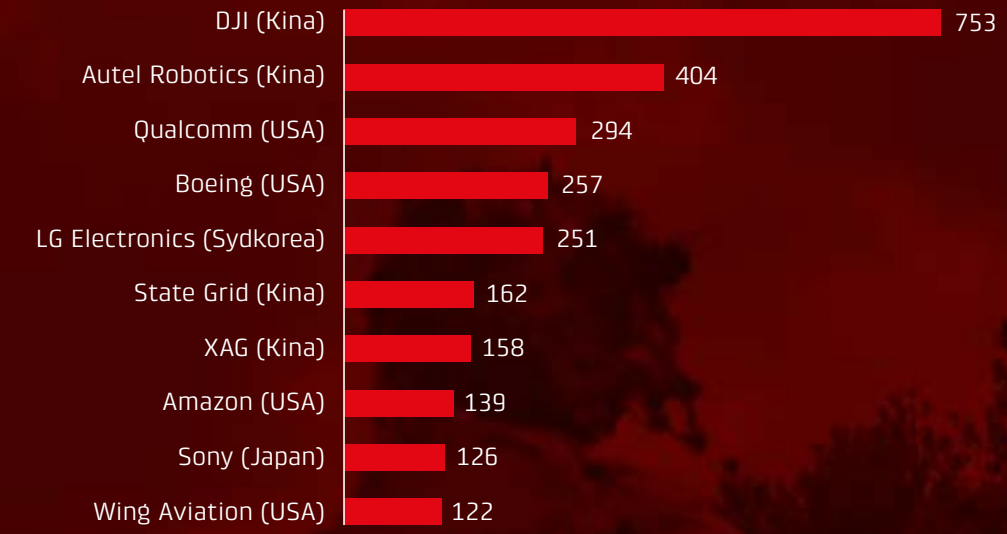
Droneinnovation

Figur 9. Mere end 40 gange så mange dronepatentansøgninger i 2020 som i 2010



Antal årlige patentansøgninger relateret til droneteknologi. Baseret på 17.150 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier.

Figur 10. Kina fører i dronekapløbet, efterfulgt af USA



Antal droneansøgninger i perioden baseret på ansøgers adresse. Baseret på 17.150 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier.

Figur 11. Mest patentsøgende lande inden for droneteknologi

Baseret på 17.150 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier.

Trend 3

Modularitet

Modularitet er den tredje trend og et designprincip, der kendes i en mange forskellige brancher. Modularitet betyder, at et system eller produkt opdeles i separate, selvstændige moduler med veldefinerede grænseflader, der kan sammensættes, som var det legoklodser. Hvert modul kan så udvikles, produceres og vedligeholdes uafhængigt af de øvrige moduler, og forskellige moduler kan sammensættes til en specifik opgave.

I forsvarsindustrien er modularitet lig med fleksibilitet, da moduler kan udskiftes eller opgraderes uden at påvirke resten af systemet. Dette letter vedligeholdelse og opdatering af systemer. Modulære design muliggør også hurtig integration af nye teknologier og kapabiliteter, selv fra forskellige producenter, da der er standardiserede grænseflader mellem modulerne.

Modularitet som tankegang gennemsyrer i stadig højere grad forsvarsindustriens tilgang til produkter, især i lyset af den tiltagende integration af systemer, som beskrevet. Når flere systemer skal kunne tale sammen, er modularitet en stærk strategi, da det giver brugeren mulighed for at til- og fravælge de moduler, der er relevante, og integrere dem i sit system.

Modularitet muliggør tilpasning til eksisterende og fremtidige systemer

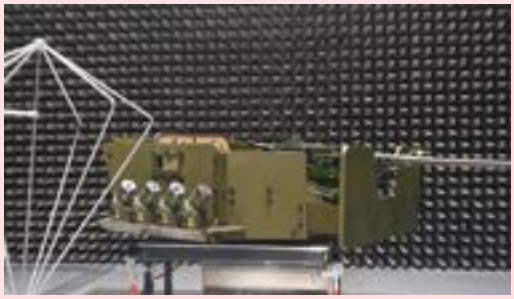
Modularitet muliggør fleksibilitet i tilpasning af nye produkter til eksisterende platforme. For eksempel opererer flere virksomheders produkter med en åben application programming interface (API), hvilket tillader nem

Modularitet er omdrejningspunktet for SIMA Innovations systemer

SIMA Innovation producerer motoriserede ringmounts og tårnløsninger, som kan anvendes til montering af forskellige våbensystemer på diverse køretøjstyper. Systemerne er baseret på et modulært princip.

Den grundlæggende ringmount-løsning er konstrueret fleksibelt, så den kan installeres på forskellige køretøjstyper. Brugere kan så vælge mellem forskellige moduler afhængigt af, hvilke systemer der skal understøttes. Dette giver mulighed for at sammensætte både enkle løsninger til få systemer og mere omfattende løsninger til flere systemer. Systemet tilbyder også forskellige grader af beskyttelse på ringmounten, som kan vælges efter behov.

For SIMA Innovation giver den modulære tilgang kunden mulighed for at sammensætte systemet til de konkrete behov på en mission. Ved at have systemerne som modulære "legoklodser" kan fartøjet udstyres til de konkrete behov på en specifik dag, og det kan ændres til dagen efter. På et tidspunkt kan trusselsbilledet fx fordre anti-drone-kapabiliteter, og dagen efter kan der være behov for at



tilføje et panserværnsmissil. Her giver den modulære tilgang fleksibilitet for brugeren.

Modularitet giver også robusthed, da beskadigede dele kan skiftes ud løbende. På den måde kan platformen hurtigere sættes i funktion igen, og den samlede levetid forlænges, da nedslidte elementer løbende kan udskiftes.

Endelig er modularitet lig fremtidssikring. Ved at have en modulær platform kan SIMA Innovation integrere nye våbensystemer, sensorer og beskyttelse, der udvikles i fremtiden. De har dermed ikke bundet sig til den eksisterende teknologi, og de har mulighed for at imødekomme de forskellige systemer, nye kunder måtte anvende eller planlægge at anvende.

integration af nye kommunikationsteknologier og sensorer. Det gør det muligt for kunderne at opgradere deres systemer med nye funktioner, efterhånden som teknologien udvikler sig. Produkterne er dermed ikke begrænset af, hvilke teknologier der allerede er på markedet, da nye sensorer og lignende kan monteres på den eksisterende platform.

Modularitet muliggør tilpasning til opgaven

At modularitet giver mulighed for tilpasning er også en vigtig fordel, da en teknologisk platform ofte skal anvendes til opgaver af forskellig karakter, hvor der er behov for forskellige funktioner. Her kan man eksempelvis udskifte

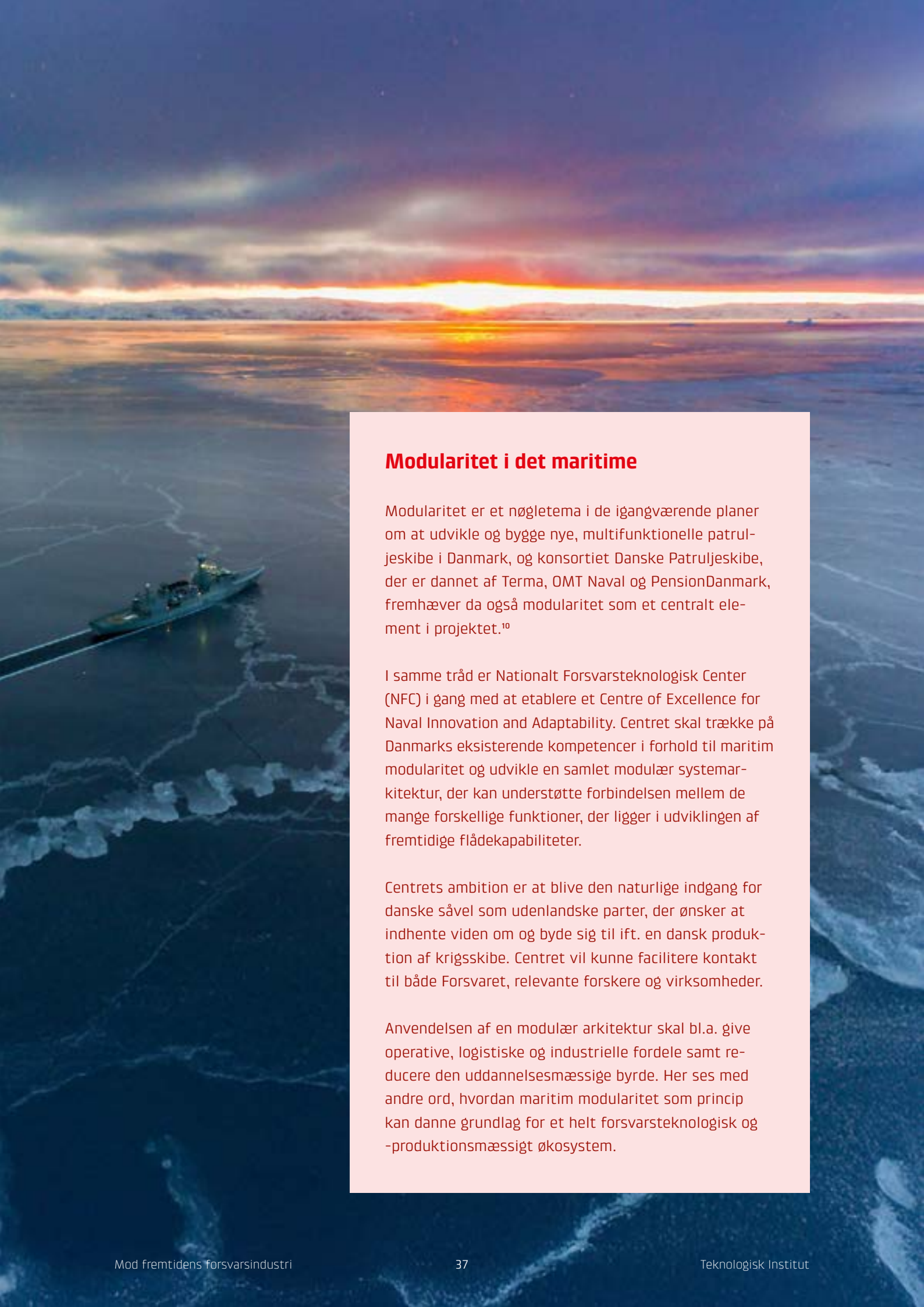
komponenter som kameraer i nogle dronesystemer afhængigt af den specifikke missions krav eller udskifte våbensystemer, så de passer til det aktuelle trusselsbillede. Denne mulighed reducerer omkostningerne, da man kan nøjes med at købe færre droner og tilpasse dem til de enkelte missioner. Derudover sparer det slid på de moduler, der kun skal bruges til nogle missioner, og det gør hele dronen lettere, end hvis den altid skulle bære samtlige moduler.

Modularitet skaber robusthed ift. vedligehold, opdatering og udskiftning

Modularitet i design understøtter robusthed i systemer, da det muliggør udskiftning og servicering af enkeltdele uden behov for at erstatte hele systemet. Dette designprincip reducerer både omkostninger og nedetid, hvilket er kritisk i forsvarsindustrien, hvor pålidelighed og hurtig reaktionsevne er afgørende.

ODU Denmark opbygger deres kabelløsninger til skibe i moduler, hvilket gør det muligt at skifte beskadigede sektioner af fiber- eller kobberkabler uden at skulle trække helt nye kabler igennem hele skibet. Det sikrer, at kommunikationssystemer hurtigt kan blive genoprettet, hvis de er blevet beskadiget. Skibe kan sågar udstyres med et sæt kabelmoduler i reserve, så de selv kan skifte beskadigede dele uden behov for nye reservedele eller teknisk specialistviden til installationen.

På samme måde bruger Systematic "containerisering" i deres softwareløsninger, der gør det muligt at opdatere dele af deres system uden at tage hele systemet offline. Det reducerer drastisk den sårbarhed, et system ellers kunne befinde sig i under systemopdateringer.



Modularitet i det maritime

Modularitet er et nøgletema i de igangværende planer om at udvikle og bygge nye, multifunktionelle patruljeskibe i Danmark, og konsortiet Danske Patruljeskibe, der er dannet af Terma, OMT Naval og PensionDanmark, fremhæver da også modularitet som et centralt element i projektet.[10]

I samme tråd er Nationalt Forsvarsteknologisk Center (NFC) i gang med at etablere et Centre of Excellence for Naval Innovation and Adaptability. Centret skal trække på Danmarks eksisterende kompetencer i forhold til maritim modularitet og udvikle en samlet modulær systemarkitektur, der kan understøtte forbindelsen mellem de mange forskellige funktioner, der ligger i udviklingen af fremtidige flådekapabiliteter.

Centrets ambition er at blive den naturlige indgang for danske såvel som udenlandske parter, der ønsker at indhente viden om og byde sig til ift. en dansk produktion af krigsskibe. Centret vil kunne facilitere kontakt til både Forsvaret, relevante forskere og virksomheder.

Anvendelsen af en modulær arkitektur skal bl.a. give operative, logistiske og industrielle fordele samt reducere den uddannelsesmæssige byrde. Her ses med andre ord, hvordan maritim modularitet som princip kan danne grundlag for et helt forsvarsteknologisk og -produktionsmæssigt økosystem.

Trend 4

Forsyningssikkerhed

De geopolitiske rammer og den teknologiske udvikling stiller nye krav til, hvordan virksomheder på forsvarsområdet driver forretning. En central trend er de øgede krav til forsyningssikkerhed. Køberne af forsvarsmateriel, om de er danske eller udenlandske, stater eller virksomheder, efterspørger i dag større og hurtigere leverancer, og de stiller flere krav til sikkerheden omkring produktionen.

Kapitlet her udfolder det øgede fokus på forsyningssikkerhed som en fjerde trend i forsvarsindustrien. Betegnelsen forsyningssikkerhed bruges bredt til at beskrive de forhold, der vedrører leverancen af produktet til rette tid og i rette kvalitet. Forsyningssikkerhed har altid

været vigtig i forsvarsindustrien, men under de aktuelle internationale omstændigheder er betydningen blot vokset, og emnet udgør derfor i dag en selvstændig trend.

Produktionshastighed og -stabilitet

Der er stor forskel på at producere krigsmateriel i fredstid og i krig. I fredstid skal der (i hvert fald i princippet) produceres tilstrækkelig ammunition og udstyr til, at der er nok på lager og til Forsvarets løbende forbrug i øvelser og træning. I krigstid er forbruget langt højere, da der forbruges langt mere ammunition på slagmarken, og udstyr, fartøjer og andet beskadiges i brug eller ødelægges af modstanderen. Når en krig først er blevet varm, stiller det derfor langt højere krav til produktionen.

Som beskrevet i afsnittet om autonomi er små droner allerede blevet en forbrugsvare på slagmarken i Ukraine, ligesom ammunition og granater. Derfor er det også en central kvalitet ved en leverandør af dronesystemer, at de kan levere hurtigt og i store mængder. Dette stiller krav til virksomhederne og deres valg af underleverandører. For den enkelte virksomhed understreger behovet for produktionsvolumen potentialet i automatisering. Mere automatiserede processer betyder potentielt, at der kan leveres flere enheder på kortere tid – og ideelt med reducerede enhedsomkostninger.

Derudover må virksomheder vælge underleverandører med omhu, så de ikke pludselig mangler centrale komponenter i deres produk-

ter. Denne faktor har fået flere danske forsvarsvirksomheder til at vælge danske samarbejdspartnere, da det gør den løbende dialog nemmere og mindsker nogle forsyningsrisici. Andre har valgt selv at stå for en større del af deres forsyningskæde for derigennem at gøre sig uafhængige af eksterne parter. Begge dele understreger behovet for at have klar styring med sin produktion og sine leverancer – selv når der kunne være billigere leverandører af komponenter i udenlandet.

En anden model er at etablere produktion nær sine største kunder. UXV Technologies har fx etableret produktion i Pennsylvania, USA, for at være tættere på det amerikanske marked og imødekomme ønsket om amerikanskproducerede produkter.

Tillid og sikkerhed

En helt central del af at være leverandør på forsvarsområdet er tillid. Og i takt med voksende geopolitiske spændinger mellem stormagterne vokser også bevidstheden om, at virksomheder kan rammes af cyberangreb, af kompromitteret udstyr fra underleverandører eller af intern industrispionage. Derfor stiller købere af forsvarsmateriel, især amerikanske, i dag

For Rival skaber partnerskaber stabilitet og troværdighed

Rival tilbyder løsninger inden for CNC-bearbejdning, herunder drejning, fræsning og finbearbejdning. Rival begyndte at levere til forsvarsindustrien omkring 2016, en udvikling der blev igangsat på grund af ustabilitet i olie- og gasindustrien, hvor Rival tidligere havde mange aktiviteter. Forsvarsindustrien blev valgt som et nyt markedssegment, da den har lignende krav til kritisk produktion, hvilket er Rivals kernekompetence.

Rivals kerneprodukter inkluderer stålkonstruktioner og panser af aluminium, plast og en bred vifte af andre materialer. Rival ser potentiale i kunstig intelligens til at optimere forskellige dele af produktionen, herunder tidsestimering, kalkulering af omkostninger og produktionsplanlægning.

En af de store udfordringer ved at levere til forsvarsindustrien er at håndtere kom-

plekse værdikæder, der spreder sig over flere lande i Europa. Rival samarbejder med forskellige underleverandører, såsom støberier og overfladebehandlere, og lægger stor vægt på processikkerhed, kvalitet og præcision. Rival foretrækker derfor også partnerskaber frem for konsortier, da de oplever, at langvarige partnerskaber giver de bedste rammer for at etablere en stabil værdikæde, der kan levere komplekse produkter effektivt.

Kvalitet betyder tillid hos Almexa

Almexa specialiserer sig i fræsning af aluminium. Almexas produkter er komponenter til bl.a. kamerahuse til fjernstyrede våbenstationer, sensorer til feltoperationer, undervandsminedetoneringsudstyr, droneudstyr og anti-drone-enheder. De leverer også komponenter til 5G-netværksenheder, der kan oprettes i områder uden netværksdækning.

For omkring 15 år siden skiftede Almexa fokus til forsvarsindustrien i forbindelse med Danmarks anskaffelse af nye jagerfly. Selvom de ikke endte med at levere til F-35'eren, specialiserede de sig i aluminium og fræsning og udvidede deres profil inden for rumteknologi og robotteknologi.

Overgangen til at blive underleverandør til forsvarsindustrien stillede høje krav til Almexas produktion. Selvom aluminiummaterialet er det samme, er tolerancerne og kravene meget specifikke på forsvarsområdet. Almexa bliver ofte auditeret af deres kunder for at sikre, at de har styr på deres forretningsgange, håndtering af information og intern kommunikation. For at få fodfæste på markedet var det afgørende at opbygge tillid med kunderne, og det skete gennem små forespørgsler, audits og gradvist større ordrer. For Almexa var deltagelse i netværk, som CenSec, også vigtig for at opbygge samarbejdsrelationer med andre virksomheder i industrien.

større krav til sikkerheden omkring produktionen. Hvis ikke de har tillid til en leverandør, får denne meget svært ved at lande en ordre.

Danske forsvarsvirksomheder har derfor stor opmærksomhed på at signalere, at de er partnere, man kan have tillid til. Terma kræver fx sikkerhedsgodkendelser for deres ansatte, og virksomheden har desuden etableret højt sikrede lokaler, der muliggør arbejde med materiale på NATOs højeste sikkerhedsniveauer. Denne type faciliteter er kostbare og afspejler de høje krav til virksomheder, der ønsker at arbejde tæt sammen med NATO-alliancen, samt den nødvendige investering for at blive en sikkerhedssamarbejdspartner.

Der er desuden en lang række internationale certificeringer, virksomheder med store forsvarsambitioner skal leve op til. Disse udstikkes af både EU og NATO og stiller krav til forskellige forhold i produktionen og produkterne. Selvom det kan være en stor investering at opnå disse certificeringer, er de adgangsgivende til at byde ind på de større internationale ordrer.

Østasiatiske komponenter

En konkret udfordring for virksomheder, der tager livtag med deres forsyningssikkerhed, er brugen af komponenter fra Østasien – konkret fra Kina og Taiwan. Det geopolitiske klima er

i dag på et punkt, hvor det er meget svært at sælge forsvarsprodukter til amerikanske kunder, hvis der er kinesiske komponenter involveret. Så selvom der måske kan være oplagte og billige underleverandører i Kina, søger flere danske virksomheder i dag alternativer for ikke at brænde potentielle transatlantiske broer.

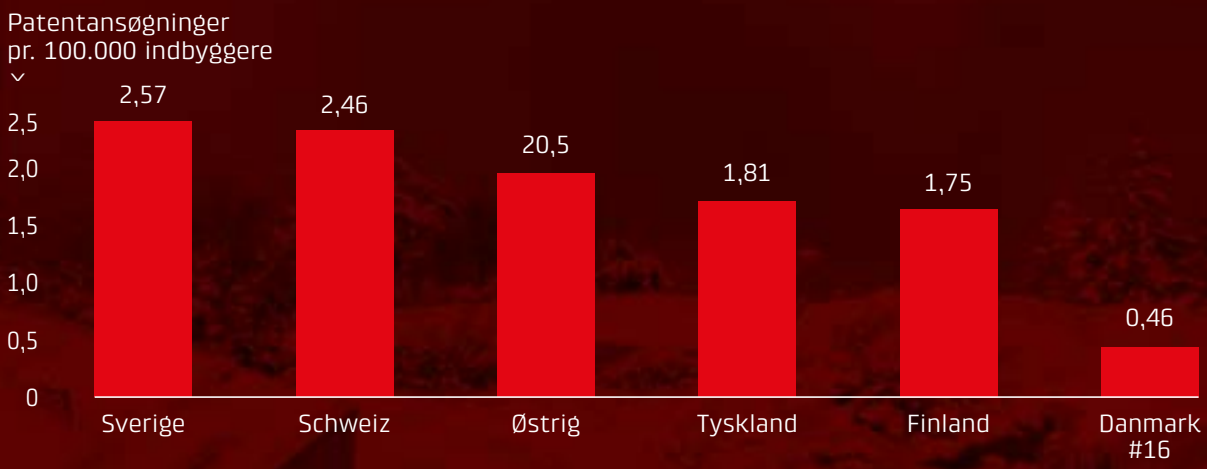
Ift. Taiwan hedder udfordringen mikrochips. I 2023 stod Taiwan for at producere mere end 60 % af verdens mikrochips og mere end 90 % af de mest avancerede mikrochips.[11] Flere virksomheder frygter, at en politisk eller sågar militær krise, der involverer Taiwan og Kina kan forstyrre den globale forsyning af mikrochips og dermed også danske virksomheders adgang til disse centrale komponenter i en lang række teknologier. Derfor afsøger flere virksomheder andre leverandører, gerne europæiske eller danske, for at sikre deres fremtidige forsyning.

EU's European Chips Act trådte i kraft i september 2023 og har til formål at styrke den europæiske produktion af mikrochips, der i 2020 udgjorde ca. 10 % af verdens samlede produktion af mikrochips.[12] Der er med andre ord også politiske vinde, der understøtter en mere lokal produktion af mikrochips. Der er dog lang vej igen, til at virksomheder ikke længere anser Taiwan for det nemme valg, når det kommer til de anvendte mikrochips' ophav. Indtil da må virksomhederne selv proaktivt opsøge alternativer.

Europæisk forsvarsinnovation

Europæisk patentkort
Kortet viser koncentrationen af de 10.000 mest citerede patenter inden for forsvarsteknologi, baseret på ansøgervirksomhedernes adresser. Rød farve indikerer en høj koncentration af ansøgninger.

Figur 12. De mest innovative europæiske lande på forsvarsområdet, 2010 – 2022



Baseret på 4.306 patentansøgninger indgivet mellem 2010 og 2022 – opgjort som patentfamilier. Europa er lige med EU inkl. Norge, Storbritannien og Schweiz.

Tabel 1. Europæiske virksomheder med flest ansøgte patenter på forsvarsområdet

Virksomhed	Land	Patenter
Rheinmetall Waffe Munition	Tyskland	285
Nexter	Frankrig	197
BAE Systems	Storbritannien	183
MDBA	Frankrig	173
Diehl Defence	Tyskland	171
Krauss-Maffei Wegmann (KMW)	Tyskland	112
Thales	Frankrig	102
Thyssenkrupp Marine Systems	Tyskland	100
Saab	Sverige	63
RUAG	Schweiz	53

Virksomhed	Land	Patenter
Airbus	Holland	51
Glock	Østrig	38
DSM	Holland	31
Safran Electronics & Defense	Frankrig	30
Atlas Elektronik	Tyskland	29
Naval Group	Frankrig	29
Heckler & Koch	Tyskland	29
DMC Global	Tyskland	28
L&O Hunting Group	Tyskland	27

Nye trends i horisonten

Denne rapport har indtil nu fokuseret på fire trends, der er vigtige for virksomhederne i dag og allerede har stor indvirkning på deres virke. Men udover de aktuelle trends er der også nogle fremtidige emner, som begynder at påvirke virksomhederne. Her er altså tale om temaer, som virksomhederne er bevidste om, men som endnu ikke for alvor er slået igennem i den danske forsvarsindustri.

I det følgende præsenteres tre fremtidige trends: "Anything as a Service", samfundssikkerhed og kvanteteknologi. Disse spiller allerede en rolle for virksomhederne, men deres potentiale er langt fra realiseret.

Anything as a Service

Betegnelsen “Anything as a Service" eller XaaS er kendt i andre dele af erhvervslivet – især blandt it-virksomheder. Det beskriver en servicebaseret forretningsmodel, hvor virksomheder sælger servicekontrakter fremfor (blot) produkter. Så i stedet for fx at sælge et computerprogram, sælges et abonnement til programmet, der i øvrigt inkluderer løbende opdateringer, oplæring til ansatte og muligheden for at sammensætte sin egen programpakke. Det klassiske eksempel er skiftet fra at købe en VHS eller DVD-film til at tegne et Netflix-abonnement. For den sælgende virksomhed flytter handlen sig her fra at være et engangssalg til at være en tidsbestemt kontrakt.

I forsvarsindustrien er denne udvikling tydeligst blandt de virksomheder, der sælger software, såsom Terma og Systematic. De har for længst adopteret en mere servicebaseret tilgang, hvor kunder indgår i længere kontrakter for til gengæld at modtage løbende systemunderstøttelse og -udvikling samt træning af personalet.

Andre dele af forsvarsindustrien er dog også begyndt at se potentiale i modellen. Nogle leverandører af fysiske produkter sælger allerede servicekontrakter som tillæg til deres produkter, hvor kunden eksempelvis løbende modtager reservedele eller regelmæssig kalibrering og serviceeftersyn af udstyret som en del af den oprindelige kontrakt. Man kunne også gå skridtet videre og tegne kontrakter på løbende forsyning af materiel eller ammunition over en årrække. Det ville også reducere behovet for lagerplads hos køberen, da denne kan afstemme kontrakten efter forbrug.

Selvom denne type kontrakter er meget almindelige i civile industrier, har den endnu ikke for alvor vundet indpas i fx det danske forsvar. Dette kan til dels skyldes en mere traditionel tilgang til budgettering, hvor det er enklere at afsætte et beløb til et indkøb en enkelt gang fremfor at tegne servicekontrakter, der skaber fremtidige udgifter. Det kan også skyldes en større opmærksomhed på at undgå "nedetid" i det civile, hvor det er mere ligetil at udregne prisen i kroner og øre på, at en given enhed er ude af funktion. Endelig kan den begrænsede brug af servicebaserede aftaler i Forsvaret skyldes, at virksomhederne har behov for kundedata for at kunne levere den bedste service, og militære organisationer er typisk meget tilbageholdende med at dele denne type data. Dermed mindskes noget af den potentielle gevinst ved servicebaserede kontrakter, da

leverandøren får ringere mulighed for løbende og forebyggende service samt for produktudvikling baseret på kundedata.

Samfundssikkerhed

En anden fremtidig trend, der gradvist er ved at blive en realitet for de danske forsvarsvirksomheder, er samfundssikkerhed som en bredere dagsorden. I de senere år – især som følge af angrebet på Nord Stream 2 i 2022 og flere NATO-allieredes meldinger om russisk hybridkrig – er beskyttelse af kritisk infrastruktur blevet et vigtigt tema i den offentlige sikkerhedsdebat. Beskyttelse af kritisk infrastruktur er da også et vigtigt tema for det nyoprettede Ministerium for Samfundssikkerhed og Beredskab i Danmark.[13]

Virksomheder i forsvarsindustrien har et potentielt voksende segment af civile kunder, der har behov for at beskytte sig imod trusler som dronespionage og -angreb. Danske virksomheder sælger allerede dronedetekteringsudstyr til lufthavne og havne, og markedet forventes at vokse i de kommende år. I 2023 blev luftrummet over Aalborg fx lukket hele tre gange på to dage, fordi der blev fløjet med droner højere end tilladt. Dette er dyrt for lufthavne, der må indstille al flytrafik i mellemtiden. Derfor er der også potentielt stor investeringsvillighed i systemer, der kan hjælpe med at identificere dronerne og dem, der styrer dem.

Samme behov for dual-use-teknologi ses i dag ved boreplatforme, havvindmølleparker og andre samfundsvigtige installationer. Udfordringen er her, at der er en uklar ansvarsfordeling og dermed et uklart mandat i forhold til, hvem der må og skal håndtere trusler imod denne type infrastruktur. Sektoransvarsprincippet i Danmark tilsiger, at det er den relevante myndighed, der har ansvar for at beskytte sine

faciliteter. Men hvem har ansvar for at afvise – eller nedskyde – en drone, der svæver rundt om en boreplatform? Det er eksempelvis ulovligt eksempelvis at bruge jammere som civil i Danmark, da disse forstyrrer signaler i luften. Derfor vil en lufthavn ikke selv kunne opsætte deciderede anti-drone-systemer til at bekæmpe ulovlig droneflyvning.

Samfundssikkerhed vil derfor først for alvor slå igennem som trend på det danske marked, når der er en klar ansvarsfordeling mellem etaterne, virksomhederne og ejerne af den kritiske infrastruktur. En egentlig sikring af kritisk infrastruktur mod eksempelvis uautoriseret droneaktivitet vil kræve enten en betydelig oprustning hos militæret og/eller politiet eller langt større beføjelser til, at civile aktører må tage hårdhændede midler i brug. Der kan dog være betydelige muligheder på udenlandske markeder med en anden lovgivning på området.

Kvanteteknologi

Kvanteteknologi rummer stort potentiale på forsvarsområdet og er derfor allerede et vigtigt emne for danske virksomheder – også selvom potentialet for de flestes vedkommende ligger et stykke ude i fremtiden. Kvanteteknologi kan opdeles i tre områder: kvantesensorer, kvantekommunikation og kvantecomputere, og European Defence Agency (EDA) afsluttede i 2023 et internationalt innovationsprojekt under ledelse af den store luftfarts- og forsvarsvirksomhed Thales, der undersøgte nogle af de forsvarsrelaterede potentialer for teknologien på alle tre områder.[14]

De første ultranøjagtige kvantesensorer er allerede i brug til varsling af vulkanudbrud samt i hjernescannere. På forsvarsområdet rummer kvantesensorer især potentiale for autonome systemer, da de muliggør meget præcis navigation i områder uden GPS-adgang på små enheder. Dette kan kombineres med såkaldt sværmeteknologi til at muliggøre autonom styring af mange droner i områder uden GPS-adgang.

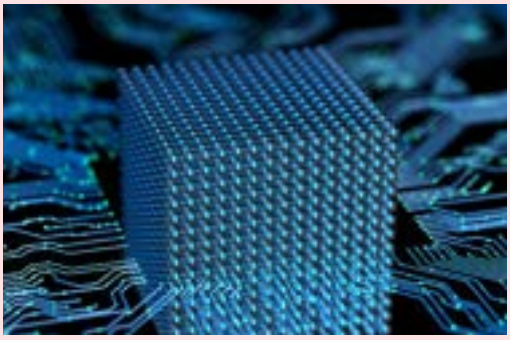
Kvantekommunikation bruger kvantemekanikkens principper til at udveksle informationer med høj sikkerhed. Der findes allerede kommercielle produkter, der trækker på teknologien, men disse er stadig meget dyre. På forsvarsområdet kan kvantekommunikation være med til at understøtte sikkerheden på kritiske systemer, fx ved at blive brugt, når der skal sendes nøgler til krypterede informationskanaler.

Hvor kvantekommunikation kan understøtte systemers sikkerhed, udgør kvantecomputere en eksistentiel trussel imod selvsamme. Kvantecomputere er det af de tre kvanteområder, der teknologisk har længst vej igen, før det for alvor slår igennem – men dets potentiale er tilsvarende enormt. Kvantecomputere vil kunne løse komplekse problemer langt hurtigere, end traditionel computerkraft og åbner dermed en række nye muligheder. På forsvarsområdet og inden for cybersikkerhed generelt truer kvantecomputere med at kunne knække gængse krypteringer og sikkerhedssystemer med hidtil uset fart og dermed gøre kritiske systemer sårbare. Kvantecomputere har derfor potentiale til for alvor at disrupte it-sikkerhed og kryptering i fremtiden, og virksomhederne følger aktivt med i, hvad det betyder for dem.

I Danmark er kvanteteknologi i dag mere et forskningsområde end et forretningsområde. Uddannelses- og Forskningsministeriet har dog udgivet en National Strategi for Kvanteteknologi, der skal gøre Danmark klar til at udvikle og anvende teknologien, og Danmark er da også allerede det land i OECD, der udgiver tredje flest forskningsartikler om kvanteteknologi i forhold til indbyggertallet.[15] Vurderet ud fra kvanterelaterede patenter er Danmark på en 14. plads i OECD, og kigger man på kvanteinvesteringer i forhold til indbyggertallet, er Danmark på en 6. plads. Der sker med andre ord meget i kvanteforskningen, og virksomhederne er derfor ved mentalt at gøre sig klar til, at teknologien kan kommercialiseres.

Terma satser på kvanteteknologi til at fremtidssikre Forsvaret

Terma, Danmarks absolut største forsvars- og sikkerhedsvirksomhed, satser strategisk på kvanteteknologi som en del af deres fremtidige innovationsportefølje. Virksomheden har identificeret kvanteteknologi som en central komponent i udviklingen af avancerede sensorer og kommunikationssystemer, der kan revolutionere detektion og informationsbehandling i militære operationer. Terma er engageret i forsknings- og udviklingsprojekter, der undersøger anvendelsesmulighederne for kvantecomputing og kvantesensorer med henblik på at forbedre præcisionen og hastigheden af dataanalyse.



Ved at investere i kvanteteknologi ønsker Terma at sikre, at deres produkter er klar til fremtidens udfordringer. Som en del af strategien arbejder Terma på at integrere kvanteteknologier i deres eksisterende systemer, hvilket skal styrke deres kapacitet til at beskytte kritisk infrastruktur og sikre national sikkerhed. Terma har oprettet en kvanteenhed og har fra efteråret 2024 ansat nye medarbejdere med ekspertise inden for kvanteteknologi og relaterede områder.

Industri 4.0 og fremtidens internationale forsvarsindustri

Integration, autonomi, modularitet og forsyningssikkerhed er centrale trends i forsvarsindustrien i Danmark, men de er ikke unikke for forsvarsindustrien. Store dele af den øvrige industri har været i gang med at gennemgå en lignende transformation, der ofte betegnes med et samlet begreb som industri 4.0.[16]

Industri 4.0 beskriver kort fortalt en sammensmeltning af det fysiske og det digitale i produktionen. Her står digital integration altså centralt, og denne er ofte betinget af modulariteten af de elementer, der integreres. Endelig bruges denne kombination af det fysiske og digitale – ofte indfanget i brugen af digitale tvillinger – til at automatisere processer og implementere effektiviserende løsninger baseret på kunstig intelligens, der trækker på de hidtil usete datamængder i produktionen.[17] C2-systemer er forsvarsteknologiens digitale tvilling, da de også skal gengive virkeligheden digitalt så præcist som muligt ud fra en række datainput, så der kan træffes informerede beslutninger om handling.

Ud over industri 4.0 kendetegnes det internationale forsvarsmarked, som andre industrier, i dag af en større grad af opsplitning mellem regionerne. Et mere protektionistisk USA lægger større vægt på at købe fra amerikanske producenter, og europæisk oprustning og usikkerhed om amerikansk NATO-engagement skaber ligeledes gunstige betingelser for opblomstringen af den europæiske forsvarsindustri.

Danske forsvarsvirksomheder lever i meget høj grad af eksport, og derfor er disse udviklinger vigtige for den fremtidige markedsadgang. Nogle virksomheder har allerede taget konsekvensen og øget deres tilstedeværelse i USA for fortsat at kunne byde sig til på det store amerikanske marked – også under mere restriktive betingelser. Her satses altså på at fastholde og udbygge det etablerede forsvarsindustrielle samarbejde med store amerikanske virksomheder, der har tæt kontakt med det amerikanske militær.

Men der ses også konturerne af en bevægelse imod større europæisk integration i fælles værdikæder, bundet op på en fælles modulær tilgang. Denne bevægelse ses bl.a. i ambitionen om det allerede omtalte danske patruljeskibsprojekt, der skal kombinere kompetencer fra flere danske virksomheder og kunne levere til hele Europa ud fra de forskellige behov, de pågældende lande har. Målet er her at etablere en samlet, modulær produktion, der ikke blot leverer platforme, der kan integreres, men også understøtter en fundamental integration af den europæiske forsvarsindustri. Denne integration kan derudover rumme EU-støtte til fælles indkøb eller produktion af udstyr og andre tiltag,

der styrker båndene mellem de europæiske forsvar, forsvarsvirksomheder og forskningen.

Det er for tidligt at sige, om de stærkere europæiske værdikæder i fremtiden vil overstige det transatlantiske forsvarsindustrielle samarbejde i volumen og betydning for danske virksomheder. Udviklingen vil afhænge af, hvordan fremtidens NATO-samarbejde ser ud (navnlig USA's fortsatte engagement i alliancen), samt om de kommende år byder på handelskrig mellem USA og Europa. Omvendt kan stormagtsrivaliseringen mellem USA og Kina (og Rusland) også føre til en styrkelse af de transatlantiske bånd, især hvis europæiske NATO-medlemmer øger deres bidrag til den militære inddæmning af Kina i Asia-Pacific. I et sådant scenarie vil stærkere militært samarbejde mellem Europa og USA også kunne resultere i større forsvarsindustrielt samarbejde – og desuden stærkere forsvarsindustrielle bånd til østasiatiske demokratier som Japan og Sydkorea.

En yderligere central faktor for fremtidens europæiske forsvarsindustri er regeringernes villighed til at realisere deres store forsvarsambitioner i fremtiden. I Danmark og udlandet er der blevet annonceret store forsvarsinvesteringer i de kommende år, men villigheden til at finde pengene vil blive prøvet, når andre politiske prioriteter banker på døren. Hvis ikke der er et solidt europæisk aftagermarked for forsvarsudstyr, vil forsvarsindustrien savne en vigtig partner. Men selv i et scenarie, hvor de europæiske lande ikke kan eller vil realisere de lovede forsvarsinvesteringer, må der forventes voksende europæisk efterspørgsel på dual-use-teknologier til beskyttelse af kritisk infrastruktur.

Endelig vil den danske og europæiske forsvarsindustris internationale fremtidige relevans afhænge af virksomhedernes evne til at levere innovative, nye teknologier, der kan omsættes til konkrete løsninger. Ifølge en rapport fra

2024 af ATV, udarbejdet af Teknologisk Institut, sakker Europa dog generelt bagud i forhold til Kina og USA, når det kommer til udvikling inden for kritiske teknologier som avanceret halvlederteknologi (semiconductors), kunstig intelligens samt robotteknologi og autonome systemer.[18] Disse teknologier er centrale i arbejdet med forsvar og sikkerhed, og fremtidens forsvarsindustri i Danmark er derfor afhængig af en vedvarende satsning på innovation i virksomhederne og på tæt samarbejde mellem industrien og den relevante forskning.

Uanset vil de virksomheder, der formår at levere integrerede og modulære systemer, der udnytter potentialet i autonomi og kunstig intelligens og er understøttet af en robust forsyningskæde, stå langt stærkere på fremtidens forsvarsmarked - om det så bliver et primært transatlantisk eller europæisk marked.

Noter

[1] IRIS Group (2024). Danmarks forsvarsindustrielle økosystem: Kortlægning og analyse af kapabiliteter, muligheder og barrierer, februar.

[2] NATO (2024). Emerging and disruptive technologies, 8 august.

[3] Nationalt Forsvarsteknologisk Center (2024). Forsvarsteknologisk forskning i Danmark, februar.

[4] For en drøftelse af forholdet mellem "integration" og "interoperabilitet" se Nisser, John (2022). Integration is the New Black: Thoughts on Future Warfare in Academic and Military Discourses. Scandinavian Journal of Military Studies, 5 (1), s. 398-411

[5] NATO (2023). Multi-Domain Operations in NATO – Explained, oktober.

[6] Forbes (2024). Next-Gen Smart Warehouses: How AI Is Shaping The Modern Supply Chain, 26 juni.

[7] For en kortlægning af aktuelle megatrends i den danske lydindustri, se Teknologisk Institut og Danish Sound Cluster (2024). "Megatrends in the Sound Industry", juni.

[8] Watling, Jack & Reynolds, Nick (2023). Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine, Royal United Services Institute, 19 maj.

[9] Axe, David (2024). In The Hottest Sector of The Ukraine War, The Ukrainians Might Deploy As Many Drones As The Russians Deploy Soldiers, Forbes, 11 marts.

[10] Danske Patruljeskibe. Fleksible og moderne patruljeskibe til søværnet.

[11] The Economist (2023). Taiwan's dominance of the chip industry makes it more important, 6 maj.

[12] European Commission. European Chips Act.

[13] Altinget (2024). Ny beredskabsminister om ændret trusselsbillede: "Det kræver, at vi får et styrket setup", 21. september.

[14] European Defence Agency (2024). QuantaQuest project explores application of quantum technologies in defence, 19 januar.

[15] Teknologisk Institut (2023). Kvanteteknologi i Danmark: Fremtiden er kvanteteknologi – hvordan kommer Danmark med? Teknologisk udsyn nr. 2, december.

[16] McKinsey & Company (2022). What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?, august.

[17] Teknologisk Institut og VisionDenmark (2024). Kreative teknologier: Teknologiske trends og forretningspotentialer i den digitale visuelle industri.

[18] ATV (2024). Kritiske teknologier: globale hotspots, europæiske perspektiver, danske muligheder, november.

TEKNOLOGISK
INSTITUT

teknologisk.dk