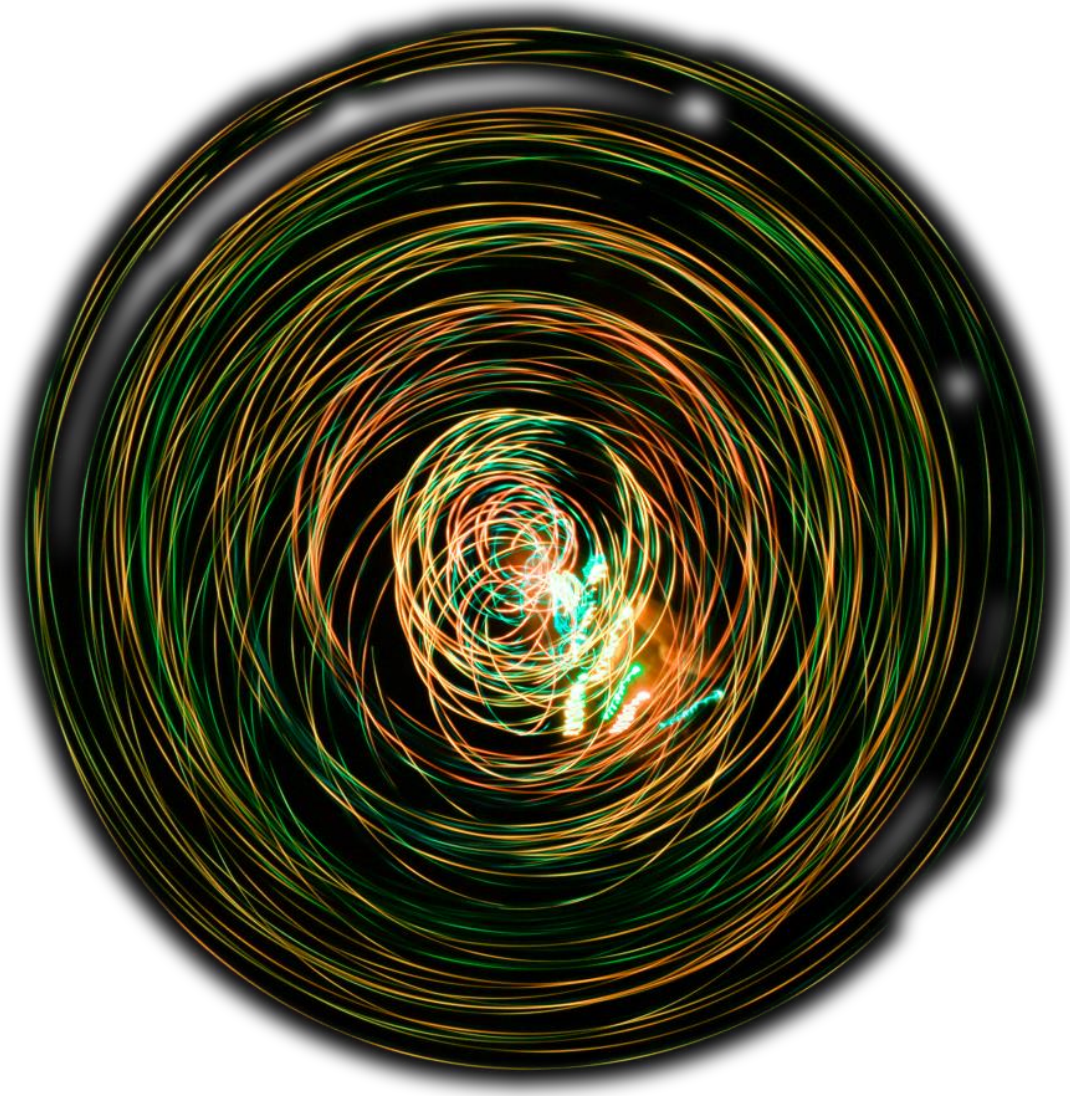
Deloitte.



Potentialet ved et styrket dansk økosystem for cybersikkerhed og -forsvar

Udarbejdet for Security Tech Space og Nationalt Forsvarsteknologisk Center

September 2024

Indhold

1. Sammenfatning

Den danske cybersikkerhedsbranche har potentiale til at blive en af Europas førende aktører inden for digital sikkerhed med mulighed for betydelig vækst. Dette kræver en strategisk indsats i hele økosystemet og investeringer i både kompetencer og avancerede teknologier samt udbygning af kapaciteten med fokus på nøglesektorer som sundhed, energi, robotteknologi og forsvar, hvor Danmark i forvejen har konkurrencefordele på det globale marked.

Denne rapport indeholder resultaterne af en kortlægning af den danske cybersikkerhedsbranche og de forventede potentialer ved at styrke det danske økosystem for cybersikkerhed og -forsvar gennem en strategisk satsning på kapacitetsopbygning med særligt fokus på branchens sikkerhedskritiske rolle i samfundet. Rapporten er udarbejdet af Deloitte for Security Tech Space og Nationalt Forsvarsteknologisk Center i perioden juli-september 2024. Analysen er baseret på en kombination af kvantitative og kvalitative datakilder, herunder et dokumentstudie af eksisterende litteratur, statistik samt interviews. Sammenfattende konkluderer analysen følgende:

Kapacitetsopbygning udgør et potentiale, men er også et akut behov

Analysen kortlægger ikke alene et kommercielt potentiale i at styrke det danske økosystem for cybersikkerhed og -forsvar, men også et akut behov. Trusselsniveauet mod Danmark er højt og komplekst, men vores forsvar vurderes at være utilstrækkeligt. Den teknologiske udvikling og stigende digitalisering i samfundet har i lang tid øget efterspørgslen efter cybersikkerhedsbranchens kompetencer og viden, men udbuddet kan ikke følge med. Vurderingen er, at vi i Danmark vil mangle op til 20.000 fuldtidspersoner med kompetencer inden for cybersikkerhed i 2030. Dertil kommer, at efterspørgslen - selv om den er stigende, ikke er på det niveau, som trusselsniveauet og omkostningerne, hvis det går galt, vil tilsige. 40 pct. af de små og mellemstore virksomheder (SMV'er) har et utilstrækkeligt digitalt sikkerhedsniveau, og i den offentlige sektor er kun 54 procent af de samfundskritiske it-systemer sikkerhedsmæssigt tilstrækkelige[1]. Den relativ store tillid i det danske samfund fremhæves af flere datakilder som en mulig forklaring på de modsatrettede forhold, at vi i Danmark har et af verdens mest digitaliserede samfund, men ikke prioriterer tilstrækkelige ressourcer til at beskytte det. Kun 5-10 pct. af SMV'ernes it-budgetter er afsat til cybersikkerhed, men vi forventer, at denne andel vil vokse til ca. 30 pct. drevet af regulatoriske krav og et mere komplekst trusselsbillede, hvor udbredelsen af Artificial Intelligence (AI), Internet of Things (IoT) og Industrielle Internet of Things (IIoT) både medfører muligheder og risici.

[1] IDA (2023): Cyber- it- og informationssikkerhed. Har Danmark de rigtige kompetencer?

”Vi er måske verdensmestre i digitalisering, men ikke i at beskytte den”

Informant i interview

Når dette er sagt, rangeres Danmark dog stadig blandt de bedste lande målt på Global Cybersecurity Index (GCI)[2]. Men udfordringer som mangel på eksperter, sårbarheder i SMV-sektoren og den stigende kompleksitet af cybertrusler kræver handling. For at fastholde og styrke denne position skal Danmark derfor investere i uddannelse, teknologi, forebyggelse af cyberangreb og koordinering og målretning af den samlede indsats, herunder særligt de mange offentligt-private samarbejder i økosystemet.

It- og cybersikkerhedsbranchen har stor betydning for dansk økonomi

Den danske it- og cybersikkerhedsbranche beskæftigede 107.330 fuldtidsansatte ved udgangen af 2023. Branchen står dermed for knap 4 pct. af beskæftigelsen i Danmark. I 2023 omsatte branchen for 313 mia. kr. Dette svarer til en andel på ca. 9 pct. af Danmarks bruttonationalprodukt (BNP). It- og cybersikkerhedsbranchen eksporterer ca. en tredjedel af sin omsætning (108 mia. kr.), og tegner sig dermed for ca. en fjerdedel af dansk industris samlede eksport. Det er svært at vurdere, hvor stor en andel af it- og cybersikkerhedsbranchen, der beskæftiger sig med cybersikkerhed, fx fordi, at det sjældent er det eneste, en it-virksomhed udbyder. Med afsæt i kortlægningen vurderer vi, at cybersikkerhedsbranchen tæller ca. 300 virksomheder. Virksomhederne i cybersikkerhedsbranchen omsætter for ca. 6,4 mia. kr., hvilket svarer til ca. 2 pct. af den samlede omsætning i hele it- og cybersikkerhedsbranchen. Knap hver 10. ansat – eller ca. 10.700 fuldtidspersoner, er beskæftiget med cybersikkerhed i it- og cybersikkerhedsbranchen. Dertil kommer 5.000-6.000 fuldtidsansatte, som arbejder med cybersikkerhed i andre brancher, ligesom specialister inden for operationsteknologier, herunder robotteknologi og IoT, også er relevante at tælle med i kompetencepuljen i lyset af cybersikkerhedsbranchens udvikling.

… og er vokset kontinuerligt i en lang årrække

Den danske it- og cybersikkerhedsbranche er karakteriseret ved relativt mange nye SMV’er, der primært er centreret i klynger i og omkring de store universitetsbyer, Aarhus og København. I takt med den teknologiske udvikling og stigende digitalisering af vores samfund er branchen vokset kontinuerligt over en lang årrække og mange nye virksomheder er kommet til. Ud af it-og cybersikkerhedsbranchens knap 17.000 virksomheder er ca. en fjerdedel etableret inden for de sidste 10 år[3]. Væksten kan særligt tilskrives en positiv udvikling for it- og cybersikkerhedsbranchen i Aarhus og København, men også i de andre universitetsbyer Aalborg og Odense har branchen oplevet en fremgang, der ligger over landsgennemsnittet. Samlet set er it- og cybersikkerhedsbranchen vokset med ca. 42 pct. fra 2019 til 2023 målt på omsætning, og branchen er dermed blandt de brancher, der er vokset mest de sidste 5 år.

Cybersikkerhedsbranchen kan vækste til dobbelt størrelse

I de kommende år vil behovet for at beskytte vores digitale infrastruktur være kilde til forsat vækst i cybersikkerhedsbranchen. Efterspørgslen efter cybersikkerhedsbranchens produkter og tjenesteydelser vurderes i øjeblikket at være for lav i forhold til trusselsniveauet; både hos virksomheder samt de statslige og kommunale myndigheder. Ny regulering, herunder EU's cybersikkerhedsdirektiv,

[2] Global-Cybersecurity-Index
[3] Særkørsel fra eStatistik

NIS2, en stigende modenhed hos virksomhedsledelser og bestyrelser samt et øget politisk fokus på forsvar, samfundssikkerhed og beredskab forventes imidlertid at få efterspørgslen efter personer med kompetencer inden for cybersikkerhed og -forsvar til at stige markant i de kommende år. Dertil kan lægges en øget efterspørgsel fra en voksende forsvarsindustri, hvor ny teknologi integreres i eller supplerer eksisterende forsvarsmateriel og -teknologi. Konkret er det vurderingen, at et acceptabelt cybersikkerhedsniveau i Danmark vil kræve 4-5 gange så mange fuldtidsansatte inden for cybersikkerhed, som tilfældet er i dag, herunder både ansatte i it-branchen og andre brancher. Den stigende efterspørgsel forventes samlet set at betyde, at cybersikkerhedsbranchen kan fordoble sin størrelse målt på både omsætning og fuldtidsansatte inden for de næste 5-10 år. Dertil kan lægges indirekte gevinster for virksomheder i andre brancher, som fx leverer input til cybersikkerhedsbranchen, samt afledte gevinster. De afledte gevinster udspringer af det øgede sikkerhedsniveau, der følger med den øgede efterspørgsel. Grundet et bedre cyberforsvar er det forventningen, at omkostningerne forbundet med cyberangreb vil falde; både direkte omkostninger, driftstab, genopretningsomkostninger samt bøder.

Potentialer for spin-in til forsvarsindustrien og Danmarks globale styrkepositioner

Den danske cybersikkerhedsbranche er i en international sammenhæng ikke særlig stor. Men branchen er relativt stærk på områder, som er vigtige i en forsvarsrettet og sikkerhedskritisk sammenhæng, herunder fx kryptologi samt kommunikation- og sensorteknologi. En væsentlig del af potentialet for cybersikkerhedsbranchen er derfor kapacitetsopbygning målrettet forsvarsindustrien, hvor spin-in af produkter og tjenesteydelser, der også anvendes i en civil sammenhæng (dual use), skal drive vækst. Heri ligger også eksportpotentialet. Den danske cybersikkerhedsbranche består af specialiserede, men relativt små virksomheder, der alene vil stå relativt svagt i den internationale konkurrence. Men ved at fokusere kapacitetsopbygningen på områder, hvor Danmark har komparative fordele på verdensmarkedet, og gennem målrettede samarbejder med fx life science-industrien og energisektoren, udvider sin globale rolle, kan den danske cybersikkerhedsbranche styrke sin rolle internationalt. Ved at arbejde mod en status som Europas digitale sikkerhedsleverandør kan Danmark samtidig styrke sin position i cyberdiplomatiet i regi af NATO og EU, hvor Danmark i forvejen nyder anerkendelse for sin indsats med at styrke cybersikkerheden.

Danmark har et sammenhængende og voksende økosystem at bygge videre på

Kapacitetsopbygning og en strategisk indsats i det danske økosystem for cybersikkerhed og -forsvar er afgørende for at leve op til NIS2-kravene og realisere branchens potentiale. Den danske cybersikkerhedsbranche beskrives som relativt lille og koncentreret i og omkring Aarhus og København. Dette skaber fordele som gode netværksmuligheder, mobilitet og stærke faglige miljøer med universiteterne i centrum, der kan tiltrække og fastholde arbejdskraft. Dog udgør de små klynger og manglen på store globale aktører en barriere for at imødekomme både den indenlandske efterspørgsel og branchens internationale ambitioner. Danmark har et mangefacetteret økosystem, der strækker sig på tværs af virksomheder, offentlige myndigheder, forsknings- og uddannelsesinstitutioner og organisationer, der arbejder for at styrke den digital sikkerhed. Samarbejdet har dog primært fokus på beskyttelse af virksomheder og kritisk infrastruktur, og mindre på kommercialisering og vækst. Derudover er det primært inden for kritisk infrastruktur, at der findes formaliseret samarbejde på tværs af aktører i økosystemet. De fleste samarbejder er uformelle og savner en samlet strategisk retning. For at optimere innovation og samarbejde i økosystemet kræves en mere koordineret og strategisk indsats, der både adresserer sikkerhedsmæssige og kommercielle mål.

Mangel på kvalificeret arbejdskraft og regulatoriske krav udgør de største barrierer
Den største barriere for at lykkes med at etablere et tilstrækkeligt cybersikkerhedsniveau og realisere de økonomiske potentialer, der er forbundet med kapacitetsopbygning i og omkring cybersikkerhedsbranchen, er mangel på kvalificeret arbejdskraft. Det gælder både profiler med tekniske og digitale kompetencer, herunder kryptologi og kvantemekanik, men også profiler, der kombinerer den tekniske og forretningsmæssige forståelse. Den demografiske udvikling er en forklaring på rekrutteringsudfordringerne. Derudover fremhæves vanskelighederne ved at tiltrække udenlandsk arbejdskraft, de relativt få kvinder i branchen og dimensionering på de videregående uddannelser som barrierer. En anden barriere er regulering, der kan begrænse markedsadgangen, øge omkostningerne og generelt udfordre konkurrencesituationen for cybersikkerhedsvirksomhederne. I en forsvarsrettet og sikkerhedskritisk sammenhæng gør høje certificeringskrav og lange godkendelsesprocedurer det svært at komme ind på markedet. Endeligt kan begrænset adgang til kapital og manglende investeringer være en barriere; særligt for SMV'er på vækstrejsen samt i markedsmodningen af nye teknologier og løsninger, der fx er et resultat af triple helix-samarbejder mellem aktører i økosystemet.

1.1. Løftestænger

Med afsæt i analysens resultater kan vi pege på følgende fem løftestænger, der kan understøtte realisering af potentialerne og sikre cybersikkerheden på samfundsplan:

Styrk uddannelsessystemet inden for cybersikkerhed: Både i form af nye uddannelser, men også ved at sikre integrere cybersikkerhed i det eksisterende udbud. Dertil kan lægges et fokus på efter- og videreuddannelse, så nuværende ansatte løbende får mulighed for at opdatere deres kompetencer til den dynamiske udvikling på området.

Gør kompetencepuljen større: Både ved at sikre bedre forudsætninger for at tiltrække og fastholde udenlandsk arbejdskraft og øge antallet af kvinder i branchen.

Let adgangen til markedet: Både ved at hjælpe cybersikkerhedsvirksomhederne med at forstå og efterleve de regulatoriske krav og opnå certificering samt i form af økonomisk støtte til vækstrejsen.

Fokuser den strategiske indsats og innovationssamarbejde i økosystemet på de forsvarsrettede og samfundskritiske områder, hvor Danmark også har komparative fordele i den globale konkurrence, herunder særligt sundhed, energi og forsvar.

Prioriter investeringer i forskning og udvikling på området, så Danmark holder sig på forkant med et stadigt mere komplekst cybertrusselsbillede og sikrer et højt fagligt miljø og kritisk masse i forskningsmiljøerne på området.

En konkret udmøntning af løftestængerne kan være en national ramme for strategisk udvikling af cybersikkerhedskompetencer. Gennem en målrettet indsats og pulje for forskning og udvikling inden for cybersikkerhed kan man understøtte et konkurrencedygtigt kompetenceudbud, og at Danmark positionerer sig som en førende udbyder af digital sikkerhed i Europa. Samme tilgang har vi set inden for udvikling af de danske styrkepositioner på fx energi- og fødevareområdet, hvor forskning og udviklingsaktiviteter samtidig understøtter en løbende tilgang af personer med de rette kompetencer i økosystemet.

2. Om rapporten

Denne rapport tegner et billede af den danske cybersikkerhedsbranche samt de potentialer og barrierer, der er forbundet med at investere i kapacitetsopbygning i branchen ud fra både et sikkerhedsmæssigt og kommercielt perspektiv.

I takt med, at nye teknologier og digitalisering breder sig og integreres i alle dele af vores samfund, bliver truslen fra cyberkriminalitet, -spionage og -terror stadig større. Et globalt scenarium, hvor risiciene ved at være digitalt forbundne oversteg gevinsterne, blev tilbage i 2015 ikke kun anset som et scenarium, men en realitet, der kaldte på øjeblikkelig handling[4].

Cybertruslen mod Danmark er i øjeblikket meget høj, hvilket fremgår af Center for Cybersikkerheds trusselsvurderinger. Truslerne kommer både fra strategisk og forretningsmæssig motiveret cyberspionage samt økonomisk motiveret cyberkriminalitet fra kriminelle organisationer. Dertil kan lægges trusler mod vores demokrati, fx gennem spredning af misinformation, samt cybertruslen som en del af hybrid krigsførelse. Som et af verdens mest digitaliserede samfund er vi særligt sårbare.

I det seneste årti er et effektivt cyberforsvar til beskyttelse af vigtige samfundsfunktioner, kritisk infrastruktur, virksomheder og borgere rykket op på den politiske agenda. Siden 2015 har vi i Danmark haft tre nationale strategier for cyber- og informationssikkerhed, regeringen har nedsat et cybersikkerhedsråd og under udarbejdelsen af denne analyse fik vi et Ministerium for Samfundssikkerhed og Beredskab, der blandt andet skal udfylde rollen som national it-sikkerhedsmyndighed. Det er forventningen – og håbet, at det nye ministerium kan være den instans, der tager ansvar for en fælles og koordineret indsats for cybersikkerhed og -forsvar i Danmark. Fraværet af en sådan instans har været noget, som implementeringen af de tidligere strategier på området har lidt under ifølge flere informanter.

Cybersikkerhed er dog også forbundet med kommercielle potentialer. Cybersikkerhedsbranchen er blandt de hurtigst voksende brancher i Danmark og udgør en voksende andel af den samlede forsvarsindustri, ligesom virksomheder og organisationer i stigende grad efterspørger cybersikkerhedsbranchens kompetencer til forebyggelse og afhjælpning af digitale trusler. Efterspørgslen forstærkes af EU's cybersikkerhedsdirektiv, NIS2 (Network and Information Security Directive 2). Direktivet indeholder retlige foranstaltninger til at øge det overordnede cybersikkerhedsniveau i EU. Knap 1.100 danske virksomheder forventes i første omgang at blive berørt af direktivet, der trådte i kraft i 2023[5]. Dertil kan lægges den

[4] Atlantic Council and Zurich Insurance Company Ltd (2015), Overcome by cyber risks? Economic benefits and costs of alternate cyber futures

[5] Ny-analyse-1079-virksomheder-pa-tvars-12-sektorer-ser-ud-til-at-blive-direkte-omfattet-af-nis2-direktivet. Lovforslaget angiver ca. 2.000 virksomheder.

kommende Cyber Resilience Act (CRA). CRA er en lovgivning, der skal styrke cybersikkerheden for produkter med digitale elementer på det indre marked i EU.

Et øget trusselsniveau kombineret med den hastige teknologiske udvikling og digitalisering i samfundet medfører gode vækstbetingelser for den danske cybersikkerhedsbranche; også udover Danmarks grænser. Men mangel på kvalificeret arbejdskraft og risikovillig kapital er nogle af de barrierer, der skal overkommes.

Den grundlæggende hypotese for analysen er derfor, at der er både sikkerhedsmæssige og kommercielle argumenter for at styrke det danske økosystem for cybersikkerhed og -forsvar, og at realiseringen af potentialerne vil kræve investeringer i kapacitetsopbygning og en strategisk indsats, der omfatter hele økosystemet.

2.1. Formål

På den baggrund er formålet med rapporten at etablere et vidensgrundlag om den danske cybersikkerhedsbranche og de økonomiske potentialer, der forventes at være forbundet med investeringer i kapacitetsopbygning på området; særligt i en sikkerhedskritisk og dual use kontekst. Med dual use menes, at branchens teknologier og tjenesteydelser kan bruges til at opfylde både civile og militære formål. Et stærkt samarbejde mellem det civile og forsvaret i forhold til cyberteknologier forventes at medføre en række samfundsmæssige gevinster i form af bedre beskyttelse af hele det danske samfund samt en styrket konkurrencekraft og videndeling. Rapporten peger desuden på de mest centrale barrierer for realisering af potentialerne samt overordnede anbefalinger til, hvordan disse barrierer kan håndteres. Konkret besvarer rapporten tre grundlæggende undersøgelsesspørgsmål:

1. Hvordan ser den danske cybersikkerhedsbranche ud i dag, herunder også økosystemet, som branchen er en del af, og samarbejdsrelationer mellem aktørerne?
2. Hvad er potentialerne ved at styrke det danske økosystem for cybersikkerhed og -forsvar gennem en strategisk satsning på kapacitetsopbygning?
3. Hvilke barrierer er der for realisering af potentialerne for den danske cybersikkerhedsbranche – og hvordan kan de håndteres?

2.2. Data og metode

De tre undersøgelsesspørgsmål har defineret vores analytiske tilgang, der består af en kombination af kvantitative og kvalitative datakilder. Fundamentet for analysen er en kortlægning af cybersikkerhedsbranchen baseret på et dokumentstudie af eksisterende litteratur og statistik.

For at sikre en bred videnskortlægning og kvalificere vores initiale forventninger om branchens udvikling samt potentialer forbundet hermed har vi anvendt Supertrends platform som supplement til vores eget desktop studie og beskrivende statistiske analyser. Platformen kombinerer artificial intelligence (AI) med ekspertudsagn til at levere datadrevne indsigter om trends og nye teknologier.

For at opnå en dybdegående forståelse af cybersikkerhedsbrancheens potentialer og barrierer har vi afholdt 10 semistrukturerede interviews med personer, som qua deres arbejde eller forskning har opnået et indgående kendskab til cybersikkerhedsbranchen i både Danmark og globalt.

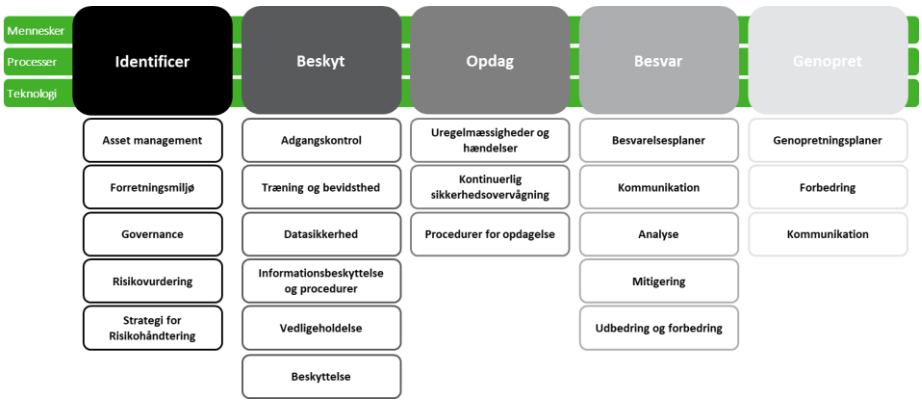
2.2.1. Afgrænsning og definitioner

Cybersikkerhed og -forsvar er et bredt område, hvorfor vores analytiske tilgang er afgrænset i forhold til analysens formål samt tids- og ressourcemæssige rammer. De fire mest centrale begreber i analysen er defineret som følger:

Cybersikkerhed

Vi definerer markedet for cybersikkerhed med afsæt i NIST CSF, der er en forståelsesramme baseret på fem fundamentale områder. Identificer, beskyt, opdag, bevar og genopret. I cybersikkerhedsbranchen er der virksomheder og ansatte, som specialiserer sig i enkelte eller flere af disse områder. På tværs af de fem områder går tre grundlæggende elementer, der skal være til stede for, at opgaverne under de fem områder kan lykkes: Mennesker, teknologi og processer. De tre elementer er internt forbundne. Teknologi fungerer ikke optimalt uden klare processer, ligesom mennesker med de rette kompetencer er afgørende for, at teknologien anvendes korrekt. Derfor er det også de tre elementer, der skal styrkes, når vi taler om en kapacitetsopbygning inden for cybersikkerhed og -forsvar.

Figur 1: Analysens forståelsesramme for arbejdet med cybersikkerhed, NIST-CSF



Note: I vores fremstilling af NIST-CSF har vi udeladt Governance som en selvstændig søjle, men vi har forholdt os til dette i forbindelse med analyse af de tre grundlæggende elementer.

Cybersikkerhedsbranchen

Vi har allerede flere gange brugt betegnelsen cybersikkerhedsbranchen. Imidlertid findes der ikke branchekoder, der entydigt definer virksomheder i cybersikkerhedsbranchen og forskellige analyser afgrænser branchen forskelligt, hvilket udfordrer sammenligninger på tværs af publikationer. I denne rapport tager vi afsæt i data om virksomheder og personer i it- og kommunikationsbranchen[6]. Ud af denne gruppe virksomheder defineres cybersikkerhedsbranchen som virksomheder, hvis primære produkter og tjenesteydelser falder inden for NIST-CSF's fem områder. Markedet for personer med kompetencer inden for it- og cybersikkerhed er dog væsentlig større, idet det også tæller personer i it-funktioner i virksomheder uden for it-branchen samt personer med en it-uddannelse, de ikke anvender.

Økosystemet

Med et styrket dansk økosystem for cybersikkerhed og -forsvar forstår vi en kapacitetsopbygning inden for cybersikkerhed i både den private og offentlige sektor samt på uddannelses- og forskningsinstitutioner. Kapacitetsopbygningen skal ske gennem investeringer i forskning og innovation samt uddannelse, tiltrækning og

[6] It- og kommunikationsbranchen tæller følgende branchekoder: 26001 Fremstilling af computere og kommunikationsudstyr mv., 46005 Engroshandel med it-udstyr, 58002 Udgivelse af computerspil og anden software, 61000 Telekommunikation, 62000 It-konsulenter mv. og 63000 Informationstjenester.

fastholdelse af kvalificeret arbejdskraft og understøttes gennem styrkede samarbejdsrelationer på tværs af aktører i hele økosystemet. Økosystemet består af virksomheder, herunder startups, i cybersikkerhedsbranchen og i branchens værdikæder, den offentlige sektor, forsknings- og uddannelsesinstitutioner samt kapitaludbydere.

Potentialet

Analysen belyser potentialerne ved et styrket dansk økosystem for cybersikkerhed og -forsvar; særligt i en sikkerhedskritisk og forsvarsrettet sammenhæng. Analysen forholder sig dog ikke til de omkostninger, der er forbundet med at realisere potentialerne. Det er dog inden for analysens rammer at fremhæve mulige indsatser, der kan løfte den danske cybersikkerhedsbranche og dermed fremme værdiskabelsen i både et samfundsøkonomisk og politisk perspektiv. Potentialerne ved et styrket dansk økosystem for cybersikkerhed og -forsvar er vurderet med afsæt i overvejende kvalitative datakilder og resultaterne har en beskrivende karakter.

Det samfundsøkonomiske potentiale kan grundlæggende inddeles i tre typer gevinster. **Direkte gevinster** er potentialet inden for cybersikkerhedsbrancheen. Fx øget omsætning og beskæftigelse. **Indirekte gevinster** er potentialet i andre brancher. Fx øget økonomisk aktivitet hos virksomheder i cybersikkerhedsbranchens værdikæder. **Afledte gevinster** er i denne sammenhæng værdien af et styrket økosystem for cybersikkerhed og -forsvar for samfundet generelt, herunder også virksomheder udenfor økosystemet og borgere. Fx værdien af et sikkert og robust internet som fundament for samhandel og økonomisk vækst i form af blandt andet reducerede omkostninger til cybersikkerhed og tab som følge af cyberangreb samt alternativomkostninger ved reduceret udnyttelse af de teknologiske og digitale muligheder. Dertil kan lægges sociale gevinster i form af øget tryghed og trivsel, samt en styrket dansk position i det internationale cyberdiplomati. Fra et ejer-/aktionærperspektiv forventer vi også, at en høj cybersikkerhed kan have positiv indvirkning på værdisætningen af en virksomhed på samme måde, som vi er begyndt at se det inden for ESG (Environment, Social, Governance) og bæredygtighed[7].

Inden for rammerne af analysen fokuserer vi primært på potentialet inden for cybersikkerhedsbranchen. Dvs. de direkte gevinster. Men en styrket cybersikkerhedsbranche vil også have multiplikatoreffekter i økonomien og højne it-sikkerheden med reducerede tab og øget tryghed til følge.

”Det er billigere at betale for forebyggelse, end at betale, når skaden er sket”

Cybersikkerhedsekspert i Deloitte

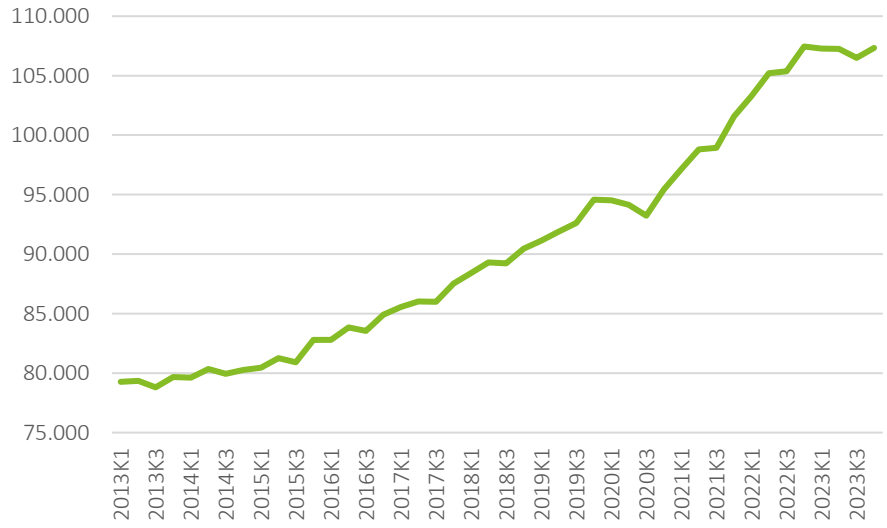
[7] Environmental-and-social-governance-in-deals-and-investment

3. Markedet for cybersikkerhed

Det danske marked for cybersikkerhed er vokset markant inden for de seneste 5 år, og selv om branchen i international sammenhæng er lille besidder den en række styrkepositioner, som i stigende grad efterspørges af en voksende forsvarsindustri.

Den danske it- og cybersikkerhedsbranche beskæftigede 107.330 fuldtidsansatte ved udgangen af 2023. Branchen står dermed for knap 4 pct. af beskæftigelsen i Danmark. Den teknologiske udvikling og stigende digitalisering af vores samfund har medført gode vækstbetingelser for it- og cybersikkerhedsbranchen, der – målt på antal fuldtidsansatte, er vokset med ca. 35 pct. de seneste 10 år.

Figur 2: Antal fuldtidsansatte i it- og cybersikkerhedsbranchen, 2013-2023



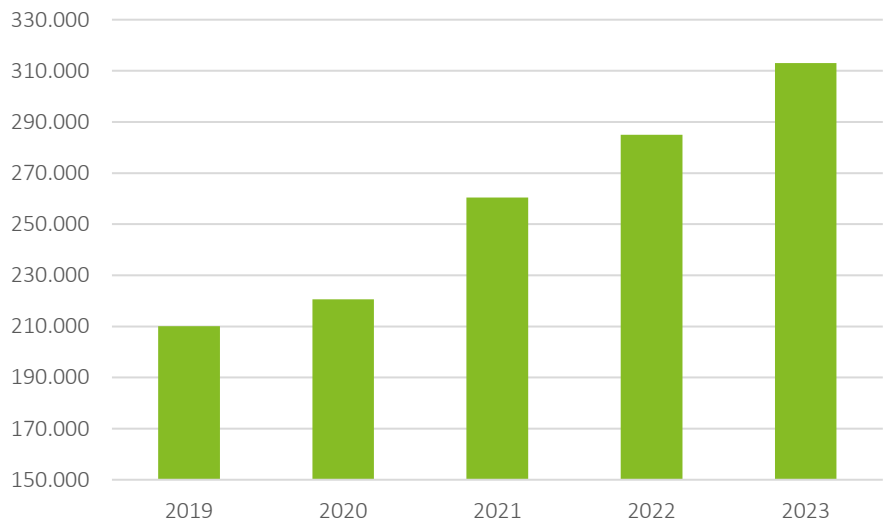
Kilde: It-Branchen på baggrund af tal fra Danmarks Statistik (It-Branchen-i-tal)

I 2023 omsatte it- og cybersikkerhedsbranchen for 313 mia. kr. Dette svarer til en andel på ca. 9 pct. af Danmarks bruttonationalprodukt (BNP). Fra 2019 og til 2023 er omsætningen i branchen steget med næsten 50 pct. Særligt under coronapandemien fra 2020 til 2021 oplevede branchen en stor stigning i omsætningen. Det er særligt fremgang i kategorierne udgivelse af computerspil og anden software samt it-konsulenter mv. der forklarer væksten i omsætningen i perioden. Engros af it-udstyr samt telekommunikation har derimod oplevet et lille fald i perioden.

Boks 1: Ansatte uden for branchen

Ifølge Eurostat udgør it-specialister 5,6 pct. af den samlede beskæftigelse, hvilket svarer til knap 162.000 personer. Heraf er ca. 107.330 personer beskæftiget i it- og cybersikkerhedsbranchen. En forskel på knap 53.000 personer, som må formodes at beskæftige sig med it, og herunder også cybersikkerhed, i andre brancher. Under antagelse af, at andelen, der beskæftiger sig med cybersikkerhed i andre brancher, er den samme, som andelen inden for cybersikkerhedsbranchen, vurderer vi, at 5.000-6.000 arbejder med cybersikkerhed uden for cybersikkerhedsbranchen.

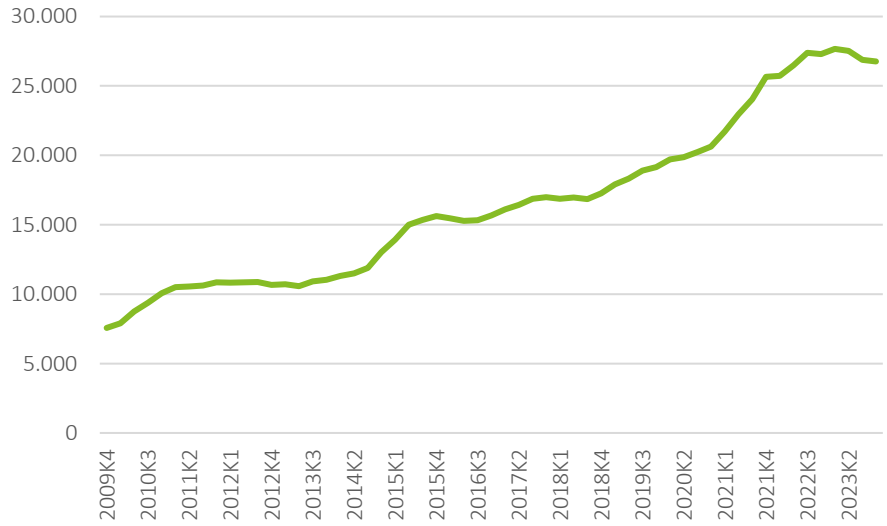
Figur 3: Omsætning i it- og cybersikkerhedsbranchen, 2019-2023, mio. kr.



Kilde: Danmarks Statistik

It- og cybersikkerhedsbranchen eksporterer lige over en tredjedel (ca. 35 pct.) af sin omsætning, hvilket svarer til 108 mia. kr. i 2023. Dermed tegner branchen sig for ca. en fjerdedel af dansk industris samlede eksport. Fra 2022 til 2023 har der været i fald i eksporten, hvilket kan forklares med relativ høj inflation og et renteniveau, der begrænser efterspørgslen på eksportmarkederne. Faldet i eksporten er dog til dels blevet opvejet af en højere indenlandsk efterspørgsel.

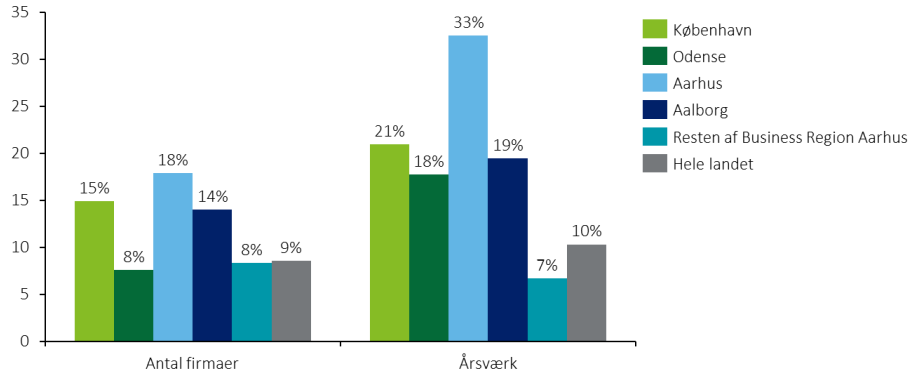
Figur 4: Eksport i it- og cybersikkerhedsbranchen, 2019-2023, mio. kr.



Note: Glidende gennemsnit, seneste 4 perioder.
Kilde: It-Branchen på baggrund af tal fra Danmarks Statistik (It-Branchen i tal - Eksport)

Den danske it- og cybersikkerhedsbranche er karakteriseret ved relativt mange nye små- og mellemstore virksomheder (SMV'er), der primært er centreret i klynger i og omkring de store universitetsbyer. Ud af it-branchens ca. 17.000 virksomheder er ca. en fjerdedel etableret inden for de sidste 10 år[8]. Fra en tidligere analyse med data for årene 2016-2021 kan vi se, at antallet af virksomheder i it-og cybersikkerhedsbranchen voksede med 9 pct. i perioden, mens antallet af fuldtidsansatte voksede med 10 pct.

Figur 5: Procentvis vækst mellem 2016-2021 for antal firmaer og fuldtidspersoner i it- og cybersikkerhedsbranchen



Kilde: eStatistik for Aarhus Kommune og Deloitte (Marts 2023): Analyse af markedet for cyber- og informationssikkerhed

Væksten kan særligt tilskrives en positiv udvikling for branchen i Aarhus og København, hvor antallet af nye it-virksomheder voksede med henholdsvis 18 pct. og 15 pct. og antallet af fuldtidsansatte voksede med henholdsvis 33 pct. og 21 pct. Men de andre universitetsbyer, Aalborg og Odense, har også oplevet markant vækst, der – særligt målt på årsværk – ligger en del over landsgennemsnittet i perioden.

Boks 2: Kort om NIS2-direktivet

NIS2-direktivet stiller krav til, at offentlige og private enheder, der leverer samfundskritiske ydelser, skal have et cybersikkerhedsniveau, der modsvarer den risiko, den pågældende enhed er udsat for. NIS2-direktivet opstiller krav til sikkerhed og beredskab for enheder der leverer kritiske tjenester, herunder digitale tjenester. NIS2 stiller krav til risikostyring, leverandørkontrol, rapportering af sikkerhedsbrud og samarbejde med nationale myndigheder og andre enheder. Direktivet dækker en bred vifte af sektorer, herunder energi, transport, finans, sundhedsvæsen og offentlige myndigheder. Formålet med direktivet er at sikre en høj fælles standard for cybersikkerhed i hele EU og styrke samarbejdet mellem medlemsstaterne og mellem de omfattede enheder. Direktivet er en del af EU's strategi for digital sikkerhed, der sigter mod at styrke EU's modstandsdygtighed mod cybertrusler og beskytte EU-borgerne på nettet.

[8] eStatistik for Aarhus Kommune og Deloitte (Marts 2023): Analyse af markedet for cyber- og informationssikkerhed

3.1. Cybersikkerhedsbranchen

Det er svært at vurdere, hvor stor en andel af it- og cybersikkerhedsbranchen, der har cybersikkerhed som deres primære forretningsområde, bl.a. fordi, at det sjældent er det eneste, en it-virksomhed udbyder. På baggrund af tidligere kortlægninger og oplysninger om virksomhedernes it-budgetter og -forbrug er det dog muligt at komme med kvalificerede estimater[9]. Vores vurdering er, at:

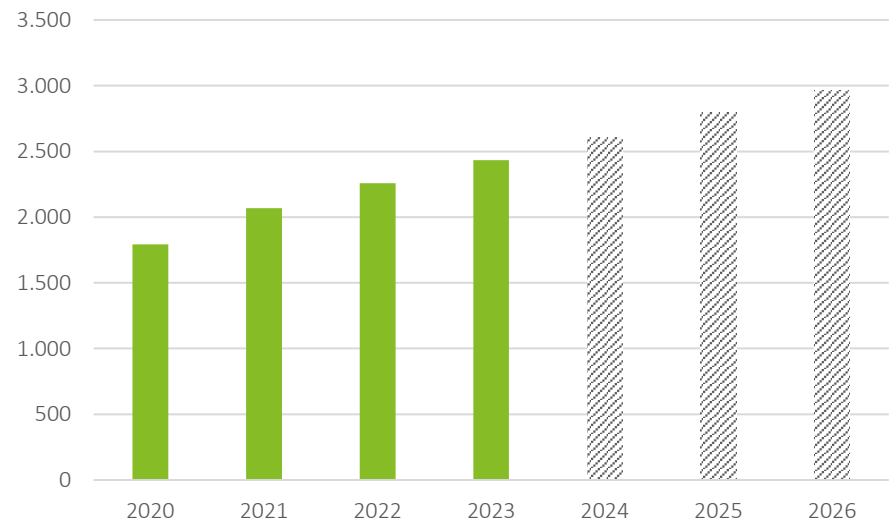
Knap hver 10. ansat – eller ca. **10.000-11.000 fuldtidspersoner** – arbejder med cybersikkerhed inden for it- og cybersikkerhedsbranchen. Dertil kommer ansatte, som arbejder med cybersikkerhed i andre brancher, fx i rådgivende revisions- og konsulenthuse samt industrivirksomheder.

Cybersikkerhedsbranchens omsætning skønnes at være ca. **6,4 mia. kr.** Et relativt beskedent beløb på ca. 2 pct. af it-branchens samlede omsætning, men et beløb, der forventes at vokse med en faktor 2-3 inden for de næste fem år.

Der findes ca. **300 virksomheder** i den danske cybersikkerhedsbranche. Dette svarer til ca. 2 pct. af det samlede antal virksomheder i it- og cybersikkerhedsbranchen.

Mens det er svært at finde tal for den samlede omsætning i cybersikkerhedsbranchen, findes der data på omsætningen inden for it-sikkerhedssoftware. Omsætningen i it-sikkerhedssoftware forventes i 2024 at være ca. 2,6 mia. kr., svarende til ca. 40 pct. af cybersikkerhedsbranchens samlede omsætning.

Figur 6: Omsætning i sikkerhedssoftware, mio. kr., 2017-2026



Note: 2024-2026 er estimater
Kilde: Supertrends på baggrund af data fra Statista

Fra 2020 til 2023 steg omsætningen af it-sikkerhedssoftware med ca. 36 pct. Tager vi estimatet for 2024 for pålydende var væksten fra 2020-2024 på ca. 46 pct. Til sammenligning var væksten i omsætningen i it- og cybersikkerhedsbranchen i samme

[9] Deloitte (2020): The Future market for Cybersecurity in Denmark og egne beregninger

periode ca. 42 pct. Det betyder, at it- og cybersikkerhedsbranchen er blandt de brancher med den største vækst i omsætningen inden for de seneste fem år.

3.2. Relative styrkepositioner

Den danske cybersikkerhedsbranche er i en international kontekst relativ lille i absolutte termer. Til sammenligning er er markedet for cybersikkerhed målt på omsætning over 100 gange så stort i USA som i Danmark, mens markedet i henholdsvis Storbritannien og Tyskland er 24 og 18 gange så stort[10]. En forklaring på den store cybersikkerhedsindustri i USA kan blandt andet findes i den netop udkomne rapport af Mario Draghi for EU Kommissionen, "The Future of European Competiveness". Her angiver Draghi fraværet af en stor forsvarsindustri som forklaring på, at Europa ligger bagefter USA, hvad angår teknologisk innovation.

> "One thing that has probably stifled technological innovation in Europe is the absence of a massive defense sector. In the US, by contrast, huge expenditures on defense-related research have played a role in the development of semiconductors, the world wide web, mobile telephony, and satellite communication and navigation"

Cheføkonom og USA-analytiker i Deloitte i resume af Draghis rapport

Netop i forhold til forsvarsindustrien udmærker den danske cybersikkerhedsbranche sig ved at have komparative fordele inden for de teknologier, som er vigtige i en forsvarsrettet sammenhæng, herunder særligt kryptologi samt kommunikation- og sensorteknologi. På disse områder har Danmark både stærke faglige universitetsmiljøer samt konkurrencedygtige virksomheder. Som eksempel kan nævnes Aarhus Universitet, der ligger i top-2 i verden inden for forskning i kryptologi.

Selv om det på tværs af flere datakilder er opfattelsen, at Danmarks generelle cybersikkerhedsniveau er udfordret, særligt i en forsvarsrettet sammenhæng og når det gælder beskyttelse af kritisk infrastruktur, ligger vi i en international sammenhæng relativ højt og vores virksomheder er generelt blevet mere opmærksomme på de digitale trusler. Andelen af danske organisationer, der har oplevet afpresning, faldt markant fra 58 pct. i 2017 til ni pct. i 2023. Til gengæld forblev andelen af phishing-angreb stabil, omkring 72 pct., i den målte periode[11]. Dette giver cybersikkerhedsbranchen og det samlede økosystem et godt fundament at bygge videre på. Hvis vi kigger på tværs af datakilder, der beskriver årsager til Danmarks relativt høje cybersikkerhedsniveau, fremhæves generelt fem årsager: En høj digitaliseringsgrad, den nationale strategi for cybersikkerhed, Center for Cybersikkerhed, offentlige-private samarbejder samt internationalt samarbejde. Interviewene har dog også afdækket en række forhold, der ifølge informanterne kan gøre styrkepositionerne endnu stærkere. Disse er kort beskrevet i Tabel 1.

[10] Deloitte (2020): The Future market for Cybersecurity in Denmark. German Trade and Invest (2023): Germany's Cybersecurity and Security Industry. Fortune Business Insights (2024): U.S. Cyber Security Market Growth - Key Industry players. National Cyber Security Center (2023): NCSC Annual Review 2023.
[11] Supertrends på baggrund af data fra Statista

Tabel 1: Danske styrker inden for cybersikkerhed og forbedringspotentialer

Styrke	Beskrivelse	Forbedringspotentiale
Høj digitaliseringsgrad	Danmark er et af de mest digitaliserede lande i verden, hvilket medfører en generel modenhed og relativ høj prioritering af cybersikkerhed i virksomheder og det offentlige.	Særligt blandt SMV'er og i den kommunale sektor vurderes investeringer i cybersikkerhed ikke at modsvare det relativt høje trusselsniveau. Samtidig er vores tillidsfulde kultur også en barriere i forhold til at sikre den nødvendige agtpågivende adfærd i samfundet.
En national strategi	Danmark har en national cybersikkerhedsstrategi (2021-2024), der sætter rammerne for en mere koordineret indsats mellem den offentlige og private sektor. Strategien fokuserer på at beskytte kritisk infrastruktur, forbedre cybersikkerhedskompetencer og styrke internationalt samarbejde. Der er en ny strategi under udarbejdelse, men midler til realisering fremgår ikke af finansloven.	Strategien er holdt på et relativt overordnet niveau. Arbejdet med cybersikkerhed i Danmark savner en masterplan med en klar ansvar- og opgavefordeling på både politisk og operationelt niveau samt et tydeligt målbillede og handlingsplan. Desuden vurderes de ca. 500 mio. kr., der er afsat i forbindelse med strategien for 2021-2024, ikke at være tilstrækkeligt til at dække investeringsbehovet på området.
Center for Cybersikkerhed (CFCS)	CFCS spiller en central rolle i at overvåge trusler mod dansk cybersikkerhed og fungerer som en rådgivende myndighed for både offentlige og private aktører. CFCS er en del af Forsvarets Efterretningstjeneste og arbejder tæt sammen med andre myndigheder og virksomheder om at håndtere cyberhændelser og beskytte kritisk infrastruktur.	Som en samlende instans, der har det overordnede ansvar for it-sikkerheden i Danmark og implementeringen af den nationale strategi, vurderes CFCS med sin placering under Forsvaret, ikke at have et tilstrækkeligt bredt fokus, endsige ressourcer til at løfte en sådan opgave. Det nye Ministerium for Samfundssikkerhed og Beredskab vil forventeligt kunne opfylde dette behov.
Offentligt-private samarbejder	Danmark er generelt god til offentligt-privat samarbejde, og der findes flere forskellige initiativer inden for cybersikkerhed. CFCS samarbejder med flere private aktører for at understøtte beskyttelsen af kritiske infrastruktur inden for blandt andet energi og vandforsyning, sundheds og den finansielle sektor. Ligesom de to opdragsgivere til denne rapport, Security Tech Space og Nationalt Forsvarsteknologisk Center, er resultatet et offentligt-privat samarbejde.	I økosystemet findes flere samarbejdsinitiativer, der skal sikre cybersikkerheden i Danmark. Det er dog primært samarbejder om beskyttelse af kritisk infrastruktur, der er formaliserede. I økosystemet findes flere uformelle samarbejder. Det er oplevelsen, at indsatsen kan drage fordel af mere koordinering med afsæt i et fælles målbillede, ligesom et større kommercielt fokus kan understøtte, at Danmark også realiserer de økonomiske potentialer, der er forbundet med fx forsknings- og udviklingsprojekter.
Internationalt samarbejde	Danmark deltager aktivt i internationalt cybersikkerhedssamarbejde i regi af EU, NATO, og andre internationale organisationer. Dette giver adgang til fælles ressourcer og bedste praksisser i kampen mod globale cybertrusler.	Danmark kan i højere grad nyttiggøre sit gode renomme i internationale forsvarssamarbejder og -alliancer til at understøtte erhvervsudvikling inden for cybersikkerhed og -forsvar.

Kilde: Dokumentstudie og interviews

4. Potentialer ved kapacitetsopbygning

Cybersikkerhedsbranchen kan vækste til dobbelt størrelse gennem en strategisk og koordineret indsats rettet mod særligt forsvarsindustrien og sikkerhedskritiske områder, men en række barrierer besværliggør vækstrejsen.

I de kommende år vil den teknologiske udvikling, fortsatte digitalisering af vores samfund og et mere komplekst trusselsbillede samt deraf følgende behov for at beskytte vores digitale infrastruktur være kilde til forsat vækst i it- og cybersikkerhedsbranchen. Selv om vi i Danmark anser os selv som verdensmestre i digitalisering, er vi ikke verdensmestre i at beskytte den. Vurderingen fra flere informanter i interviewene er, at efterspørgslen efter cybersikkerhedsbranchens produkter og tjenesteydelser er for lav i forhold til trusselsniveauet; både hos virksomheder samt de statslige og kommunale myndigheder. Særligt beskyttelsen af kritisk infrastruktur inden for den finansielle sektor, vandforsyning samt energi- og sundhedsområdet giver anledning til bekymring. Men forventningen er også, at dette vil ændre sig. Således forventes ny regulering, herunder EU's cybersikkerhedsdirektiv, NIS2, og den kommende CRA, en stigende modenhed hos virksomhedsledelser og bestyrelser samt et øget politisk fokus på forsvar, samfundssikkerhed og beredskab at øge efterspørgslen efter cybersikkerhedsbranchens produkter og tjenesteydelser. Dertil kan lægges en øget efterspørgsel fra forsvarsindustrien, hvor ny teknologi integreres i eller supplerer eksisterende forsvarsmateriel, ligesom spirende startup-miljøer i særligt Aarhus og København, hvor nye virksomheder stimulerer efterspørgsel og bidrager til vækst gennem udvikling af nye innovative løsninger med afsæt i fx AI, IoT og IIoT.

4.1. Det økonomiske potentiale

På baggrund af analyse af implikationerne af de regulatoriske krav og interviews er det vores vurdering, at et acceptabelt cybersikkerhedsniveau i Danmark vil kræve 4-5 gange så mange fuldtidsansatte inden for cybersikkerhed, som tilfældet er i dag, herunder både ansatte i it-branchen og andre brancher. I øjeblikket allokerer SMV'erne 5-10 pct. af deres it-budgetter til cybersikkerhed, mens andelen hos de større virksomheder i højrisiko for cyberangreb inden for fx finans, energi og sundhed anvender 10-20 pct. af deres it-budgetter på cybersikkerhed. Dette er i overensstemmelse med internationale studier, der viser, at virksomheder generelt anvender 10-15 pct, af deres it-budgetter på cybersikkerhed. I de kommende år er det forventningen, at virksomhederne vil bruge relativt mere på cybersikkerhed i både absolutte og relative termer. Konkret er det forventningen, at virksomhederne vil bruge mellem 2-3 gange så mange ressourcer på cybersikkerhed, som tilfældet er i dag, inden for de næste 5-10 år. Dvs. generelt vil andelen af it-budgetterne, der allokeres til cybersikkerhed, stige til ca. 30 pct. Samtidig forventer vi, at væksten i cybersikkerhedsbranchen vil udgøre en stigende andel af væksten i den samlede it- og cybersikkerhedsbranche. Dertil kan lægges øgede investeringer i beskyttelse af kritisk infrastruktur mod cyberangreb samt spin-in muligheder til forsvarsindustrien

På den baggrund vurderer vi, at den danske cyberesikkerhedsbranche kan vækste til dobbelt størrelse inden for de kommende 5-10 år. Forventningerne til den danske cybersikkerhedsbranche i 2030 er derfor:

20.000 – 22.000 fuldtidsansatte **ca. 13 mia. kr. i omsætning**

Dermed er forventningerne til den danske cybersikkerhedsbranche på niveau med forventningerne til den globale cybersikkerhedsindustri, der forventes at vokse med årlige vækstrater i omsætning på 10-12 pct. frem mod 2030[12].

4.2. Afledte gevinster

Hvis cybersikkerhedsbranchen vækster vil det have afsmittende effekt på virksomheder i andre brancher gennem input-outputrelationer. Fx kan der forventes indirekte gevinster for virksomheder i andre brancher, som leverer input til cybersikkerhedsbranchen. Dertil kommer afledte gevinster.

De afledte gevinster udspringer af det øgede sikkerhedsniveau, der følger med den øgede efterspørgsel. Grundet et bedre cyberforsvar er det forventningen, at omkostningerne forbundet med cyberangreb vil falde. Cyberangreb er forbundet med store omkostninger, der generelt kan inddeles i fem typer, og som et øget sikkerhedsniveau kan reducere:

1. **Direkte økonomiske tab**, fx som følge af ransomware-angreb, der kan koste virksomheder millioner af kroner i løsepenge eller tab af data. Den gennemsnitlige løsesum i et ransomware-angreb vurderes at være ca. 27 mio. kr.[13]
2. **Omkostninger ved driftstab**, fx grundet nedetid, hvor virksomheder ikke kan operere normalt. Den gennemsnitlige omkostning ved en datalækage vurderes at være ca. 30 mio. kr. pr. hændelse[14].
3. Genopretningsomkostninger til genopbygning af systemer og sikkerhedsinfrastruktur i form af fx ny software, opdatering af sikkerhedssystemer og ansættelse af specialister til at løse problemet.
4. **Reputationsskader** i form af tab af kunder, markedsandel og fremtidige forretningsmuligheder grundet tab af kundetillid og omdømme.
5. **Bøder** for overtrædelse af persondataforordningen (GDPR) eller andre sikkerhedslove.

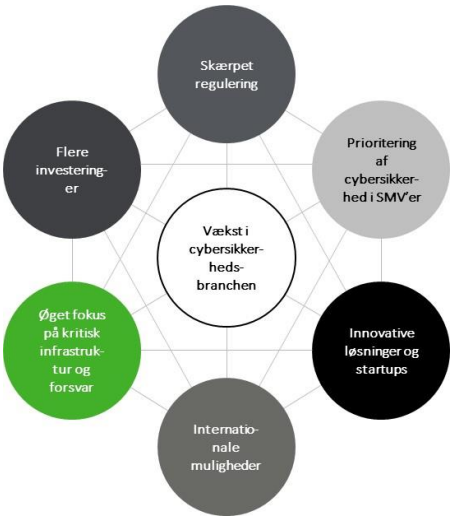
Derudover skal også fremhæves værdien af den øgede tryghed i samfundet som et højere sikkerhedsniveau alt andet lige forventes at medføre.

4.3. Realisering af potentialerne

Figur 7 illustrerer seks drivere for vækst i den danske cybersikkerhedsbranche. Datamaterialet bag analysen tillader os dog at komme et skridt dybere. Som nævnt er den danske cybersikkerhedsbranche i en international sammenhæng ikke særlig stor. Men branchen er relativt stærk på områder, som er vigtige i en forsvarsrettet og sikkerhedskritisk sammenhæng, herunder særligt energi- og sundhedssektoren.

Siden krigen i Ukraine vokser forsvarsindustrien igen, og en væsentlig del af potentialet for cybersikkerhedsbranchen er derfor spin-in af produkter og tjenesteydelser, der også anvendes i en civil sammenhæng (dual use). Det er også gennem denne tilgang, at eksportpotentialet skal realiseres. Den danske

Figur 7: Vækstdrivere for den danske cybersikkerhedsbranche



[12] Baseret på blandt andet Statista, Grand View Research and MarketsandMarkets
[13] The Manifest
[14] IBM (2023): Cost of a Data Breach Report 2023

cybersikkerhedsbranche består af specialiserede, men relativt små virksomheder, der alene vil stå svagt i den internationale konkurrence. Men ved at fokusere kapacitetsopbygningen på områder, hvor Danmark har komparative fordele på verdensmarkedet, og gennem spin-in til fx life science-industrien og energisektoren udvider sin globale tilstedeværelse, kan den danske cybersikkerhedsbranche styrke sin rolle internationalt.

Ved at specialisere sig inden for udvalgte sektorer, og hvor store udfordringer skal løses, er det samtidig forventningen, at den danske cybersikkerhedsbranche vil have nemmere ved at tiltrække forsknings- og udviklingsmidler fra virksomheder og organisationer inden for de pågældende sektorer i både ind- og udland og indgå strategiske samarbejdsaftale med disse samt opnå finansiering fra EU. Som eksempel kan fremhæves en dansk cybersikkerhedsvirksomhed, som har indgået et partnerskab med en life-science virksomheden, der udvikler løsninger til bekæmpelse af vira og bakterier, med henblik på at styrke eksporten i Norden.

Der findes allerede en del forskning om udvikling af innovationsklynger, som en strategisk baseret og målrettet kapacitetsopbygning - både i forhold til investeringer, uddannelse og forsknings- og udvikling, med fordel kan tage afsæt i. Fx har MIT Lab for Innovation Science and Policy udviklet rammeværk for, hvordan innovation og samskabelse i økosystemer kan styrkes og videreudvikles på ryggen af eksisterende styrkepositioner[15].

Boks 3: Betydning af kapacitetsopbygning for Danmarks internationale position

Med en øget investering i kapacitetsopbygning inden for cybersikkerhed er det vurderingen, at Danmark kan styrke sin position i det internationale cyberdiplomati i regi af NATO og EU og dermed påvirke cybersikkerhedspolitikker og forsvarsstrategier. En proaktiv tilgang til cybersikkerhedsområdet understøtter vores forpligtelse til at sikre kritisk infrastruktur i overensstemmelse med NATO's og EU's målsætninger. Ved aktivt at bidrage til NATO's og EU's cybersikkerhedsinitiativer kan Danmark samtidig styrke sin geopolitiske indflydelse og sikre, at vores nationale interesser afspejles i de bredere internationale sikkerhedsdagsordener. Deltagelse i internationale cyberforsvarsøvelser og -projekter styrker Danmarks operative parathed og viser vores kapaciteter, hvilket kan føre til vigtigere roller i fremtidige NATO- og EU-sikkerhedssamarbejder. Som eksempel kan næves Danmarks deltagelse i Locked Shields 2024, der er en international cybersikkerhedsøvelse, der afholdes årligt af NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). I EU-regi investeres i disse år massivt i opskaleringen. Cyber ventes at blive et centralt satsningsområde i næste fase af EU's forsvarsfond, EDF, fra 2028-2033. Med en rettidig indsats har Danmark mulighed for at medtænke EU's indsats og tage en større rolle i defineringen af fælles europæiske prioriteter. Med tilslutningen til EU's forsvarssamarbejde deltager Danmark fra maj 2023 i det forstærkede samarbejde på forsvarsområdet (PESCO). Det er desuden besluttet at Danmark skal søge om optagelse i første række i to PESCO-projekter, herunder EU Cyber Emergency Respons teams. Det rejser spørgsmål om, hvorfra de deltagende eksperter kan komme. Her ses der muligheder for samtænkning med forskningsmiljøerne, både for at sikre større bæreflade for de europæiske engagementer, og for at sikre bedre hjemtag af viden og adgang til de europæiske partnere. På NATO siden er cyberstøtten en central del af støtten til Ukraine.

[15] Budden & Murray (2019): An MIT Approach to Innovation: eco/systems, capacities & stakeholders

4.4. Barrierer for vækst

Den danske cybersikkerhedsbranche beskrives af de fleste informanter som relativt lille og koncentreret i klynger omkring særligt Aarhus og København. Dette giver fordele i form af blandt andet gode muligheder for netværk og mobilitet internt i branchen samt et stort kendskab til hinanden, ligesom de lokale faglige miljøer med universiteterne i centrum kan understøtte tiltrækning og fastholdelse af arbejdskraft. Omvendt er de relativt små klynger og fraværet af store globale aktører en barriere i forhold til at imødekomme både den indenlandske efterspørgsel samt branchens internationale ambitioner. Kapacitetsopbygning i industrien samt en strategisk indsats, der omfatter hele økosystemet, vurderes derfor at være helt afgørende, hvis Danmark som minimum skal leve op til NIS2, hvilket der vil være høje forventninger til i lyset af det kommende EU-formandskab, og samtidig realisere de potentialer, der er forbundet med en styrket dansk cybersikkerhedsbranche. På tværs af datakilder har analysen kortlagt følgende barrierer for vækst i den danske cybersikkerhedsbranche:

Mangel på kvalificeret arbejdskraft

Den største barriere for at lykkes med at etablere et tilstrækkeligt cybersikkerhedsniveau og realisere de økonomiske potentialer, der er forbundet med kapacitetsopbygning i og omkring cybersikkerhedsbrancheen, er mangel på kvalificeret arbejdskraft. Vurderingen er, at vi i Danmark vil mangle 10.000[16] og måske helt op til 15.000-20.000 fuldtidspersoner med kompetencer inden for cybersikkerhed i 2030[17]. Det gælder både profiler med tekniske og digitale kompetencer, herunder kryptologi og kvantemekanik, men også profiler, der kombinerer den tekniske og forretningsmæssige forståelse. Den demografiske udvikling er en forklaring på rekrutteringsudfordringerne, men derudover kan fremhæves vanskeligheder ved at tiltrække udenlandsk arbejdskraft som følge af dansk lovgivning, de relativt få kvinder i branchen (mindre end en tredjedel i it- og cybersikkerhedsbranchen er kvinder[18]) og adgangsbegrænsninger på it-uddannelserne som forklarende faktorer. I forlængelse heraf skal også fremhæves vigtigheden af ikke kun at fokusere på kvantitet, men også kvalitet. Den mere komplekse trusselsbillede stiller høje krav til de ansatte i cybersikkerhedsbranchen, og i den forbindelse ytrer flere informanter bekymring for, om den eksisterende pulje af it-specialister besidder de rigtige kompetencer.

Regulering

Barriererne for cybersikkerhedsbranchen fra regulering er mangefacetterede. Som nævnt er regulering med til at drive den efterspørgsel, der skal understøtte væksten i cybersikkerhedsbranchen. Men samtidig er regulering også en hindring for vækst. Danske virksomheder står over for stigende krav til regelefterlevelse i takt med implementering af ny regulering (fx NIS2, CRA og DORA). Dette kan påvirke markedsadgangen, forsinke produktudviklingsprocesser samt øge "time-to-market" og driftsomkostningerne med deraf følgende negative implikationer for virksomhedernes konkurrencesituation. Desuden er markedsadgang vanskelig for virksomheder, der ikke er i stand til at opfylde høje certificeringskrav, især i kritiske sektorer som forsvar, finans og energi. I en forsvarsrettet sammenhæng fremhæver flere informanter barrierer i form af lange og krævende processer for godkendelse af underleverandører til forsvarsindustrien.

Adgang til kapital

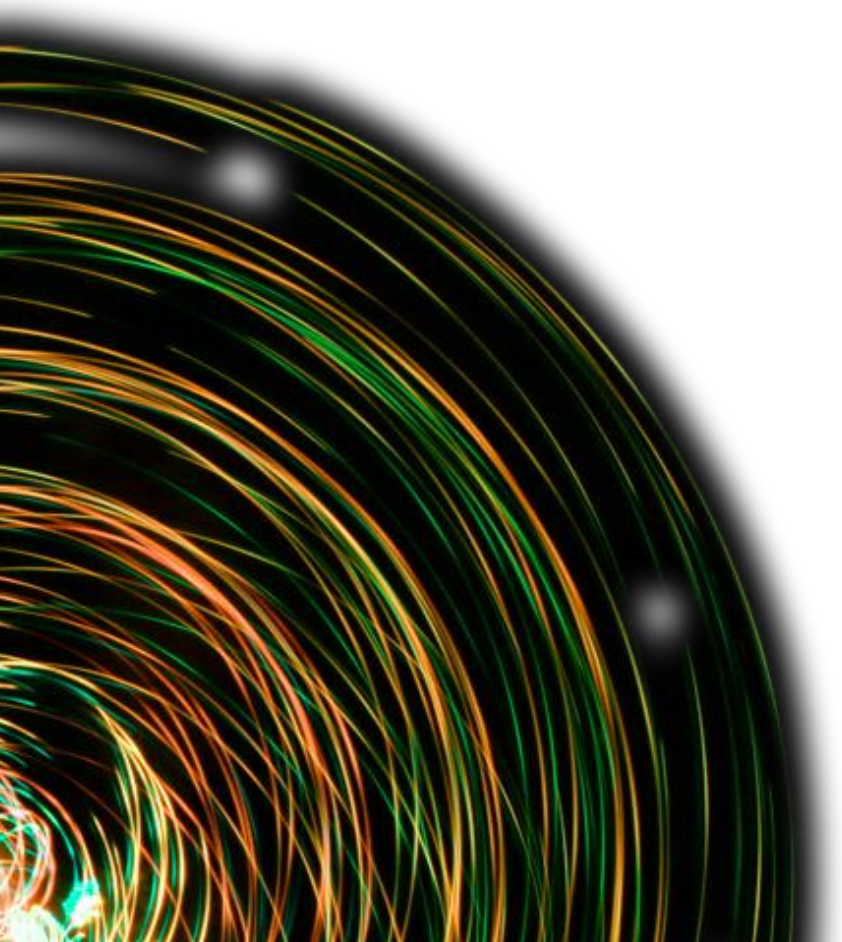
Etablering og skalering af virksomheder kræver kapital. Det samme gælder modningsprocessen af innovative løsninger fra forskning- og udviklingsstadiet til

[16] Security Tech Space eget estimat
[17] IDA (2023): Cyber- it- og informationssikkerhed. Har Danmark de rigtige kompetencer?
[18] It-Branchen-i-tal

markedet. Går vi et skridt tilbage er det desuden vigtig, at vi løbende investerer i forskning og udvikling på området, så vi holder os på forkant med et stadig mere komplekst cybertrusselsbillede og fastholder vores faglige styrkepositioner. Men adgangen til kapital, og særlig risikovillig kapital opleves som en barriere. Særligt når eksisterende løsninger skal skaleres til nye markeder, og når nye løsninger skal i markedet. Industriens Fond vurderes i den forbindelse at have spillet en vigtig rolle i udviklingen af den danske cybersikkerhedsbranche. Hvis potentialerne skal realiseres, er det vurderingen, at der er behov for mere risikovillig kapital i økosystemet.

Lav efterspørgsel

Endelig er det en barriere - eller risiko, at efterspørgslen forbliver uændret. Særligt i SMV-segmentet, hvor høje omkostninger, lav risikobevidsthed og manglende prioritering kan forhindre de nødvendige investeringer i cybersikkerhed.



5. Økosystemet

Danmark har et sammenhængede økosystem for cybersikkerhed og -forsvar og dermed et solidt fundament at bygge videre på i indsatsen for at forsvare os mod cybertrusler og realisere de økonomiske potentialer, som et styrket økosystem også medfører. Men mangel på arbejdskraft og risikovillig kapital kan få fundamentet til at slå revner.

Kortlægningen af det danske økosystem for cybersikkerhed og -forsvar tager afsæt i MIT' beskrivelse[19]. I deres analyser af innovation, består økosystemer af fem aktørtyper, der i denne sammenhæng kan defineres som 1) virksomheder i cybersikkerhedsbranchen og 2) i branchens værdikæder, 3) den offentlige sektor, 4) forsknings- og uddannelsesinstitutioner samt 5) kapitaludbydere. Inden for og mellem aktører i økosystemet findes de grundlæggende elementer mennesker, teknologi og processer, jf. også Figur 1.

Danmark har et sammenhængende og mangefacetteret økosystem på tværs af virksomheder, myndigheder og forsknings- og uddannelsesinstitutioner samt en række organisationer og organer, der arbejder for at styrke Danmarks digitale sikkerhed. Økosystemet er særligt udviklet i og omkring de store universitetsbyer. Med sammenhængende mener vi, at der i alle dele af systemet findes erfarne og/eller konkurrencedygtige aktører, der har stort kendskab til hinanden og markedet, ligesom der også er knyttet samarbejdsrelationer på tværs af sektorer. Men samarbejdet beskrives også som fragmenteret og ukoordineret, hvilket medfører overlappende mandater, og koblingen mellem myndighedssiden som øverst ansvarlig for it-sikkerheden i Danmark og økosystemet, der repræsenterer det operationelle niveau, savner et strategisk ophæng.

Offentligt-private samarbejder er relativt udpræget i det danske økosystem for cybersikkerhed og -forsvar. Dette indikerer gode *processer* i økosystemet. Det formaliserede samarbejde mellem aktører har primært fokus på at styrke it-sikkerheden i virksomheder og organisationer og beskytte kritisk infrastruktur i en situation med et stadigt mere komplekst trusselsbillede. De triple helix-inspirerede samarbejder, der typisk udspringer fra universiteterne, har i højere grad sigte på løsninger forbundet med et økonomisk potentiale, der kan realiseres med et større kommercielt fokus og en bedre adgang til kapital.

I forhold til det grundlæggende element *teknologi* udmærker økosystemet sig ved komparative fordele inden for løsninger, der er særligt relevante i en forsvarsrettet og sikkerhedskritisk sammenhæng, og inden for hvilke universiteterne også har etableret stærke faglige miljøer. Til gengæld er økosystemet udfordret på udbudssiden (*mennesker*). Adgangen til kvalificeret arbejdskraft er en af de største barrierer for vækst i cybersikkerhedsbranchen. Derudover ligger der en indsats i at

[19] Budden & Murray (2019): An MIT Approach to Innovation: eco/systems, capacities & stakeholders

sikre finansiering til vækstrejsen og til den forskning og udvikling, der skal styrke og udbygge de eksisterende styrkepositioner. En del af disse midler skal komme fra offentlige midler og fonde. Særligt et statsligt lederskab, også økonomisk, vurderes at være vigtig for realisering af de strategiske målsætninger, der blandt andet forudsætter deltagelse i europæisk og internationale partnerskaber. Men derudover er det også forventningen, at den globale forsvarsindustri vil investere store beløb i forskning og udvikling inden for cybersikkerhed, hvilket kan komme den danske branche til gode.

Figur 8: Det danske økosystem for cybersikkerhed og -forsvar

Figur 8 skitserer det danske økosystem for cybersikkerhed og -forsvar[20]. Nedenfor har vi kort beskrevet de væsentligste aktørgrupper, herunder *eksempler* på aktører i de respektive kategorier, samt processer og teknologi.

5.1. Aktørgrupper

Virksomheder i cybersikkerhedsbranchen

Ca. 300 virksomheder kan kategoriseres som cybersikkerhedsvirksomheder. Hovedparten af virksomhederne er SMV'er og en stor del af virksomhederne er startups. De nye virksomheder arbejder med innovative løsninger inden for områder som AI-drevet sikkerhed og automatisering af trusselsdetektion. Udover SMV'erne tæller ø kosystemet også en række store virksomheder, der har cybersikkerhed som en del af en større produktportefølje, fx it-virksomheder, virksomheder i forsvarsindustrien samt konsulenthuse.

Forsknings- og uddannelsesinstitutioner

Forskning og uddannelse spiller en afgørende rolle i det danske økosystem for cybersikkerhed og -forsvar. **Aarhus Universitet** (AU) etablerede omkring 1990 en forskergruppe i Kryptografi og Cybersikkerhed. Denne gruppe er i dag i top-2 i verden i forskningen på området. Forskerne er fx involveret i at formulere fremtidens standarder for "post quantum" kryptografi. AU har samtidigt uddannet et større antal kandidater og PhD'er med speciale i kryptografi og cybersikkerhed. **Danmarks Tekniske Universitet** (DTU) var også tidligt ude og etablerede cybersikkerhedsforskning og -uddannelse.

[20] Økosystemets internationale relationer samt investeringer fra aktører i andre lande er ikke inkluderet.

De tilbyder specialiserede kurser, og samarbejder med industrien om forskningsprojekter. Fra 2020 har DTU udbudt en ingeniørkandidatuddannelse i Cyberteknologi. **Aalborg Universitet** (AAU) i København fulgte i 2021 efter, og lancerede en ingeniøruddannelse med fokus på cybersikkerhed. AAU har desuden en styrkeposition indenfor kommunikationssystemer og sensorer. Universitetet står for træning af Cyberlandsholdet, i samarbejde med forskere fra flere danske universiteter og AAU leverer desuden input til CFCS' Cybersikkerhedsråd. **It-Universitetet i København** (ITU) har også cybersikkerhed som et af sine fokusområder, og fokuserer blandt andet på forskning, der kombinerer den tekniske og organisatoriske dimension. **Syddansk Universitet** (SDU) har i samarbejde med Forsvarsakademiet udviklet en Master in Intelligence and Cyber Studies, ligesom de under Center for Industriel Software er ved at opbygge uddannelsestilbud i Cybersikkerhed. En vigtig spiller er også Alexandra Instituttet, der er et dansk GTS (Godkendt Teknologisk Serviceinstitution) Institut; en nonprofit forsknings- og teknologivirksomhed, der arbejder med anvendt forskning og udvikling inden for it og digital teknologi. Alexandra Instittuttet har fx et lab, der fokuserer på cybersikkerhed, og leverer både anvendt forskning og konsulentydelser på området. Endelig udbyder erhvervsakademierne og erhvervsskolerne også uddannelser med kursuselementer indenfor cybersikkerhed.

Offentlige myndigheder

Flere offentlige aktører spiller en central rolle i at sikre og regulere cybersikkerhed på nationalt plan. **Center for Cybersikkerhed (CFCS)** er en af de vigtigste institutioner med ansvar for Danmarks nationale cybersikkerhed. CFCS blev oprettet under Forsvarets Efterretningstjeneste og overvåger landets kritiske it-infrastruktur. CFCS arbejder tæt sammen med både offentlige og private aktører og udgiver årligt rapporter om trusselsbilledet. De udadvendte og rådgivende dele af CFCS' opgaver bliver fremadrettet overført til det nyoprettede **Ministerium for Samfundssikkerhed og Beredskab**, der fremadrettet får det overordnede ansvar for it-sikkerheden i Danmark. Samtidig bliver **Ministeriet for Digitalisering** styrket med et øget fokus på den offentlige digitalisering. Derudover kan fremhæves **Digitaliseringsstyrelsen**, der arbejder for at styrke it-sikkerhed i den offentlige sektor og blandt borgerne og har ansvar for at udvikle nationale strategier for it-sikkerhed og digitalisering. I forlængelse heraf kan nævnes **Datatilsynet**, der som tilsynsmyndighed for databeskyttelse og GDPR spiller en vigtig rolle i at sikre, at virksomheder og organisationer overholder reglerne for datasikkerhed og privatliv. Endeligt skal fremhæves de mange kommuner og offentligt ejede virksomheder, herunder forsyningsselskaber, der er blandt de største mål for samfundsskadelige cyberangreb.

Kapitaludbydere

Inden for cybersikkerhedsbranchen fremhæves **Industriens Fond**, som en vigtig samarbejdspartner og kapitaludbyder. Desuden kan fremhæves **Innovationsfonden** og en række erhvervsdrivende fond, hvoraf **Novo Nordisk Fonden o**g fondens støtte til Gefion supercomputeren kan nævnes som eksempel. Generelt opfylder økosystemet de betingelser, der skal være til stede for at tiltrække mere risikovillig kapital – særligt i den tidlige vækstfase, herunder mulighed for store afkast, om end med høj risiko, innovative løsninger og teknologier, skalerbarhed og markedspotentiale. Derfor er det forventningen at kapitalfonde mv. vil have stigende interesse for branchen, særligt, i samspil med fx forsvarsindustrien.

5.2. Processer og teknologi

Der findes flere etablerede samarbejdsrelationer og -processer i økosystemet, hvoraf udvalgte initiativer er fremhævet nedenfor.

Offentligt-private samarbejder

Der er en stærk tradition for offentligt-private samarbejder om cybersikkerhed i Danmark. **D-mærket** er et cybersikkerhedsmærke for SMV'er, som er et resultat af et samarbejde mellem offentlige myndigheder og private aktører. Mærket hjælper virksomheder med at opnå og signalere høje standarder inden for it-sikkerhed. **Cybersikkerhedsrådet** er et rådgivende organ, der består af medlemmer fra både den offentlige og private sektor. Rådet arbejder for at fremme samarbejde og koordinering mellem aktørerne i cybersikkerhedslandskabet. Endeligt kan også fremhæves opdragsgiverne til denne rapport; **Security Tech Space** (STS) og **Nationalt Forsvarsteknologisk Center** (NFC). STS er skabt for at styrke cybersikkerheden i virksomheder og for at skabe vækst og udvikling indenfor området, mens NFC er en ny konstruktion, der i lyset af Ukrainekrigen og den stigende politiske usikkerhed skal mobilisere universiteter og GTS'er (Godkendt Teknologisk Service) over en bred kam med henblik på at løfte både Forsvaret og forsvarsindustrien teknologisk.

Brancheorganisationer

Brancheorganisationerne **DI Digital, DI Forsvar og Sikkerhed** og **Dansk Erhverv** spiller en vigtig rolle i at samle virksomheder om fælles initiativer og dialog om cybersikkerhed. I forlængelse heraf skal også nævnes **Dansk it**, **It-Branchen** og **IDA**, som også varetager virksomhedernes og de ansattes interesser i branchen.

Netværksplatforme

En række events og netværksplatforme bringer aktørerne i økosystemet sammen for at dele viden og styrke samarbejdet. **Copenhagen Cybercrime Conference (C3)** er en årlig konference, hvor eksperter fra både Danmark og udlandet diskuterer de nyeste trends og udfordringer inden for cybersikkerhed. **DigitalLead** er en national klynge for digital teknologi, der fungerer som et netværk og et samarbejdsforum for aktører, der arbejder med digitale løsninger. Derudover kan nævnes **CenSec**, der er den danske innovationsklynge for forsvars-, rum-, og sikkerhedsindustrien.

Teknologi

Igennem rapporten har vi løbende beskrevet, at den danske cybersikkerhedsbranche har nogle teknologiske styrkepositioner på særligt det sikkerhedskritiske og forsvarsrettede område. Disse omfatter særligt kryptologi, netværkssikkerhed og detektion af skadelig/uønsket aktivitet, malwareanalyse, authentication og adgangskontrol, beskyttelse af fortrolige data samt softwareverifikation. I forhold til læring og samarbejde på tværs af aktører i økosystemet er det værd at fremhæve, at flere informanter også påpeger vores styrke i at undervise i teknologi, fx brug af virtuelle laboratorier til data-generering og træning.

Boks 4: Om opdragsgiverne

Nationalt Forsvarsteknologisk Center er en ny konstruktion, der i lyset af Ukrainekrigen og den stigende politiske usikkerhed skal mobilisere universiteter og GTS'er over en bred kam med henblik på at løfte både Forsvaret og forsvarsindustrien teknologisk. Inden for cybersikkerhed er der masser af kompetencer, som kan anvendes bedre, både for dansk sikkerhed, men også for EU og NATO. NFC har igangsat en række projekter inden for bl.a. kvante-sikret kommunikation og sikring af Forsvarets egne cybersikkerhedssystemer.

Security Tech Space er skabt for at styrke cybersikkerheden i virksomheder og for at skabe vækst og udvikling indenfor området. Initiativet samler forskere, virksomheder, myndigheder og andre organisationer for at udvikle partnerskaber og løsninger mod cybertrusler. En væsentlig del af indsatsen er arbejdet for at etablere Cyber Campus Denmark, som har til formål at uddanne næste generation af eksperter, fremme samarbejde mellem industri og forskning samt styrke Danmarks evne til at forsvare sig mod hybridkrig.

Deloitte.