CYBER CONSCRIPTION IN DENMARK

- An evaluation of the relevancy of cyber conscription to enhance IT-security in organisations

Mads Kærulf Bornholdt
Frederik Andreas Hentze
Andreas Ravnsbæk
Casper Gottschalck Stormark

Faculty: The Faculty of Social Sciences and Humanities
Department: Department of Politics and Society
Program: Master of IS management
Date: 31 May 2024

AALBORG UNIVERSITY

STUDENT REPORT

AALBORG UNIVERSITY

The Faculty of Social Sciences and Humanities
Study board for Politics and Society
Fibigerstræde 1-3
9220 Aalborg East
https://www.politics-society.aau.dk/

Title:

Cyber conscription in Denmark

- an evaluation of the relevancy of cyber conscription to enhance IT-security in organisations

Project:

10th semester, Master's thesis

Project period:

February 2024 - June 2024

Project group:

4-ITL, group 4

Participants:

Mads Kærulf Bornholdt
Frederik Andreas Hentze
Andreas Ravnsbæk
Casper Gottschalck Stormark

Supervisors:

Christian Ravn Haslam

Signatures:

Mads Kærulf Bornholdt
bornholdt@outlook.com

Frederik Andreas Hentze
frederikhentze1996@gmail.com

Andreas Ravnsbæk
andreasravnsbaek@gmail.com

Casper Gottschalck Stormark
casper@stormark.dk

Number of pages: 80

Finished: 31st of May, 2024

The content of the report is freely available, but publication (with indication of source) may only take place by agreement with the authors.

Resumé

Abstract: Cyberspace and the digitalization of vulnerable data is intertwined like never before. Denmark is one of the most digitalized nations in the world, and with an increasing level of threat towards both the private and public sector's digital assets, cyber security and cyber resiliency is a must-have. This study will, in cooperation with'The Signal Regiment' from the Danish Army, investigate how Denmark's cyber conscription program can potentially aid in strengthening IT security in private and public organizations. The investigation is based on user evaluation from the perspective of organizational leaders, who employ Danish cyber conscripts. The collected data is processed and analyzed using a mixed-method design, encompassing qualitative semi-structured interviews, cluster interviews, observational study and surveys. The study's findings show conformity between the cyber conscripts' real-world skills, educational profile and current organizational demands. However, it also shows both disparity and correlation between what the cyber conscript program and what the user organizations deem relevant. While the respondents agree that cyber conscripts have sufficient technical skills, they are more interested in their educational profile and mindset rather than in a specific technical skillset. The right profile is hard to come by, whereas technical skills can be acquired. The latter being something the cyber conscripts have shown themselves adept at. Based on our findings, three recommendations are put forward: Establishing further cyber education / specialization within the Danish Army; and establishing career tracks targeting educated cyber conscripts. These should be across private, NCO, and officer levels; and shifting the educational focus away from an 'ambassadorial role'.

The study concludes that the Danish cyber conscript program does aid in raising IT-security within the organizations that participated in the study, and has a lot of potential as a civilian and military educational track.

Forord

Dette speciale er udarbejdet som afslutning på 10. semester på kandidatuddannelsen i IT-Ledelse på Aalborg Universitet i foråret 2024. Specialet er udarbejdet i samarbejde med Føringsstøtteregimentet, der er hovedsamarbejdspartner. Derudover indgår en række militære og civile organisationer, der har bidraget med unik og værdifuld indsigt. Yderligere har vi nydt deltagelse af en stor del nuværende og tidligere cyberværnepligtige, der har bidraget med tid, viden og indsigt. En stor del af denne kontakt er faciliteret gennem *'Foreningen for Danske Cyber Alumner'* (FDCA). Slutteligt har alle myndighedsniveauer i Forsvarets organisation bidraget med unik viden om den nationale cyberindsats. Specialet henvender sig først og fremmest til specialets samarbejdspartnere hos Føringsstøtteregimentet, og kan bidrage til deres forståelse for, om Forsvarets Cyberværnepligt opleves relevant hos de organisationer, som ansætter de cyberværnepligtige efter endt værnepligt. Derudover kan specialet indgå som anvendelsesgrundlag til fremtidige evalueringer af cyberværnepligten.

Vi vil gerne rette en stor tak til Føringsstøtteregimentet for et godt og konstruktivt samarbejde, og for deres store gæstfrihed på kasernen. Ligeledes vil vi gerne takke FDCA og de cyberværnepligtige for at hjælpe os med besvarelse af spørgeskema, og for at tage godt imod os under øvelser. Tilsvarende vil vi gerne takke de mange respondenter hos aftagerorganisationerne, som både har besvaret spørgeskema, men også taget ekstra tid ud af kalenderen for at komme med velreflekterede besvarelser under interviews, og som har budt os velkommen i deres organisation. Vi vil også gerne takke de myndighedsorganisationer, som under pressede og ellers typisk forbeholdne vilkår, var villige til at lade sig interviewe.

Sidst, men ikke mindst, vil vi gerne takke specialevejleder Ph.D. Christian Ravn Haslam for kyndig og konstruktiv vejledning, og for hans store engagement, indlevelse og interesse i vores speciale.

Indhold

Kapitel 1

Indledning

Danmark er et digitalt foregangsland (Regeringen, 2021, s. 4). Gennem gentagne undersøgelser på tværs af anerkendte internationale agenturer, rangerer Danmark ofte i top, og i den seneste officielle måling fra Europa Kommisionen, indtager Danmark en placering som det næstmest digitaliserede land i EU. Samme gør sig gældende i subkategorien *Integration of digital technology*, der omhandler virksomheders brug af teknologi (European Commision, 2022, s. 19). Den udprægede brug af teknologier, det digitaliserede samfund og mængden af forbundne systemer, skaber udviklings- og konkurrencefordele for både det offentlige og private Danmark. Samtidigt skaber disse fordele også sårbarhed overfor misbrug og nedbrud, der kan have alvorlige økonomiske og samfundsmæssige konsekvenser (Regeringen, 2018b).

Cybertrusler som begreb er ikke et nyt fænomen, men siden 2012 er der sket en kraftig udvikling i trusselsbilledet fra cyberspace, samt en øget kompleksitet i digitalt distribuerede angreb (Forsvarsministeriet, 2023, s. 6). Truslen er rettet mod alle dele af samfundet, og kan true statens sikkerhed, organisationer, virksomheder og privatpersoner. Forsvarets Efterretningstjeneste vurderer således truslen fra både *cyberspionage* og *cyberkriminalitet* til højeste kategori: *"Meget Høj"* og vurderer, at cybertruslen er en af de alvorligste trusler mod Danmark (Regeringen, 2021, s. 4 & 9). Siden årtusindskiftet har der været stort fokus på fordelene ved at digitalisere samfundet. Det er sket gennem 6 konkrete digitaliseringsstrategier. Den beskyttende del, de *Nationale Cyber- og Informationsstrategier*, er dog stadig et nyere tiltag fra 2015, og pr. 2024 på 3. udgivelse. Formålet med cyber- og informationsstrategierne er at skabe mere sammenhængskraft gennem en systematisk og koordineret indsats indenfor cybersikkerhed (Regeringen, 2018b, s. 13).

Der ses en tidsmæssig udvikling, hvor der i første strategi fokuseres på IT-sikkerhed og udbredelse af ISO27001 standarden i Staten, mens tredje og seneste udgave har fokus på cyberresiliens, som nationalt udtrykkes som robusthed. Robusthed er ét af fire strategiske fokuspunkter i den seneste nationale strategi. Robusthed, som tilsvarer resiliens, opfattes i den Nationale Cyber- og Informationssikkerhedsstrategi som værn mod samfundskritiske systemer under cyberhændelser, eller angreb mod kritiske IT-systemer under opretholdelse af drift.

Robusthed forstås bredere end sikkerhed, og omfatter områder som ledelse, viden, standardisering, analyse og overblik (Regeringen, 2021, s. 19-21). Det bredere fokus skal skabe bedre forudsætning for cyberresiliens. Det vurderes nødvendigt i lyset af en kraftig stigning i IT-kriminalitet, og at 40 % af SMV'erne i Danmark har et utilstrækkeligt sikkerhedsniveau ift. deres risikoprofil (Regeringen, 2021, s. 19).

I 2012 oprettes *Center for Cybersikkerhed* (Herefter CFCS), der agerer national IT-sikkerhedsmyndighed under Forsvarets Efterretningstjeneste. CFCS opprioriteres kraftigt i forbindelse med Forsvarsforliget 2018, hvor der afsættes 1,4 mia. samt 0,5 mia. i reserve til cyberområdet (Regeringen, 2018a, s. 11). Af forligsteksten fremgår et særligt fokus mod *"styrket rådgivning og vejledning med særligt fokus på samfundsvigtige sektorer, herunder i forhold til myndigheder og virksomheder"* samt oprettelse af et døgnbemandet nationalt cybersituationscenter (Regeringen, 2018a, s. 10). I praksis betyder placeringen af CFCS under FE, at cyberindsatsen placeres under Forsvarsministeriets ansvarsområde. På trods af betragtelige tiltag, er der et uforandret højt trusselsniveau gennem flere år (FE, 2020, s. 39), (FE, 2022, s. 40), (FE, 2023, s. 37). I 2022 rapporteres det i PwC Cybercrime survey, at 51 procent af danske CXO og IT-fagfolks virksomheder har været udsat for mindst én cybersikkerhedshændelse indenfor de seneste 12 måneder. Derudover er 63 procent af de adspurgte mere bekymrede for de cybertrusler deres virksomheder udsættes for nu, end for 12 måneder siden (PWC, 2022, s. 5 & 12).

Truslen mod det offentlige og private Danmark er reel og konkret, og der efterspørges i stigende grad kompetencer, der kan imødegå denne. Blandt flere forskellige tiltag, indfører Forsvaret i 2020 en helt ny uddannelse, Forsvarets cyberværnepligt, der skal *"bidrage til at styrke cybersikkerheden og træne de værnepligtige i at sikre sig mod trusler fra cyberspace"* (Forsvaret, 2023b). Formålet med cyberværnepligten er, *"at styrke Forsvarets og samfundets beskyttelse mod cybertrulser i fred, krise og krig"* (Se bilag [G3], s. 1). Cyberværnepligten indføres indledningsvist i 2020 som en 3-årig forsøgsordning med årlig uddannelse af 32 cyberværnepligtige (Forsvaret, 2023b, s. 2), og er en grunduddannelse indenfor cybersikkerhed. Ordningen bliver permanent fra sommeren 2023. Cyberværnepligten har haft stort fokus og megen omtale, men er aldrig blevet evalueret i forhold til om tiltaget skaber værdi for aftagere af cyberværnepligtige, eller hvorledes de cyberværnepligtiges kompetencer er relevante. Evaluering af, hvorvidt cyberværnepligtige skaber værdi for aftagerne, er undersøgelsens omdrejningspunkt, hvilket kommer til udtryk igennem problemformuleringen.

1.1 Problemformulering

Med afsæt i indledningen, har dette afsnit til formål at frembringe undersøgelsens problemformulering, samt dertilhørende underspørgsmål. Besvarelsen af de tre underspørgsmål, samt fortolkning og diskussion af besvarelsen, vil være grundlag for at kunne besvare problemformuleringen fyldestgørende. Undersøgelsens problemformulering er følgende:

> *Hvorledes opleves Forsvarets Cyberværnepligt som relevant for at højne IT-sikkerheden ved aftagerorganisationer?*

1.1.1 Underspørgsmål

Relevansen af cyberværnepligten undersøges med afsæt i uddannelsesbeskrivelsen, bilag [G3], samt uddannelsespræsentation ved Føringsstøtteregimentet, bilag [G1]. Uddannelsesskitse fremgår af figur 1.1. Jf. figuren har de cyberværnepligtige efter endt uddannelse to muligheder: *Ansættelse i Forsvaret inden for IT og Cybersikkerhed* eller *Civile uddannelses- og jobmuligheder*. Overgangen til *Totalforsvarsreserven* gør sig automatisk gældende for alle typer af værnepligtige, og fravælges derfor som en del af undersøgelsen. Dette efterlader tre primære aftagergrupper af cyberværnepligtige efter endt uddannelse: *Forsvaret*, *Civile uddannelsesinstitutioner* og *Civile organisationer*. Disse tre grupper betegnes samlet herfra *aftagere*, og udgør brugerne af cyberværnepligten. Som det fremgår af figur 1.1, bidrager uddannelsen til tre overordnede mål: *Ambassadører for god cyberadfærd*, *Basal cyberbeskyttelse* og *IT/cybersikkerhedskompetencer der kan bygges videre på*. Basal cyberbeskyttelse anses som værende en kombination af forståelse for rollen som ambassadør og IT/cybersikkerhedskompetencer, og undersøges derfor ikke igennem et separat underspørgsmål. Undersøgelsen vælges desuden også at rette fokus mod de cyberværnepligtiges personlige profil, eftersom de cyberværnepligtiges unikke personlige profil var i tale ved uddannelsespræsentation. Aftagergrupperne og målene for uddannelsen danner i kombination udgangspunkt for undersøgelsens tre underspørgsmål:

1. *Hvordan vurderes cyberværnepligtiges kompetencer og personlige profil af aftagerorganisationer?*
2. *Hvordan er forholdet mellem cyberværnepligtiges kompetencer og profil, og aftagerorganisationernes kompetence- og profilbehov?*
3. *Hvordan manifesteres rollen som ambassadør for god IT-sikkerhed i praksis?*

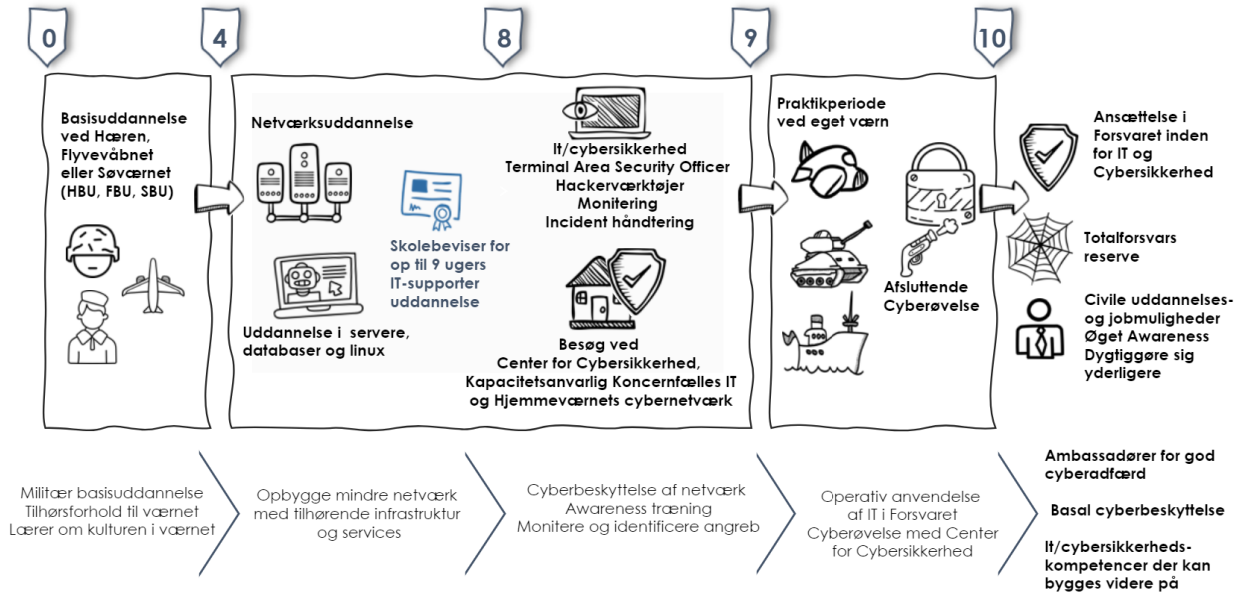
Til besvarelse af hvert af de tre underspørgsmål, udarbejdes et undersøgelsesdesign, som findes i afsnit 1.3. Undersøgelsesdesignet tager udgangspunkt i, og begrænses naturligt af, undersøgelsens case. Af denne grund findes i kommende afsnit en casebeskrivelse indeholdende cyberværnepligtens baggrund og formål, samt en beskrivelse af Forsvarets organisationsstruktur.

1.2 Casebeskrivelse

Dette afsnit har til hensigt at beskrive undersøgelsens case, samt hvordan problemformuleringen og underspørgsmålene afgrænses heraf. Indledningsvist beskrives Forsvarets Cyberværnepligt, som undersøgelsens case retter fokus mod. Herefter forefindes en kort indflyvning til Forsvarets organisationsstruktur, der kan bidrage til at rammesætte casen for læseren uden indgående kendskab til Forsvarets opbygning, som ses i princip-skitse, figur 1.2. Dette er relevant i forhold til casens afgrænsninger, hvilke beskrives afslutningsvist i afsnittet.

1.2.1 Bag om cyberværnepligten

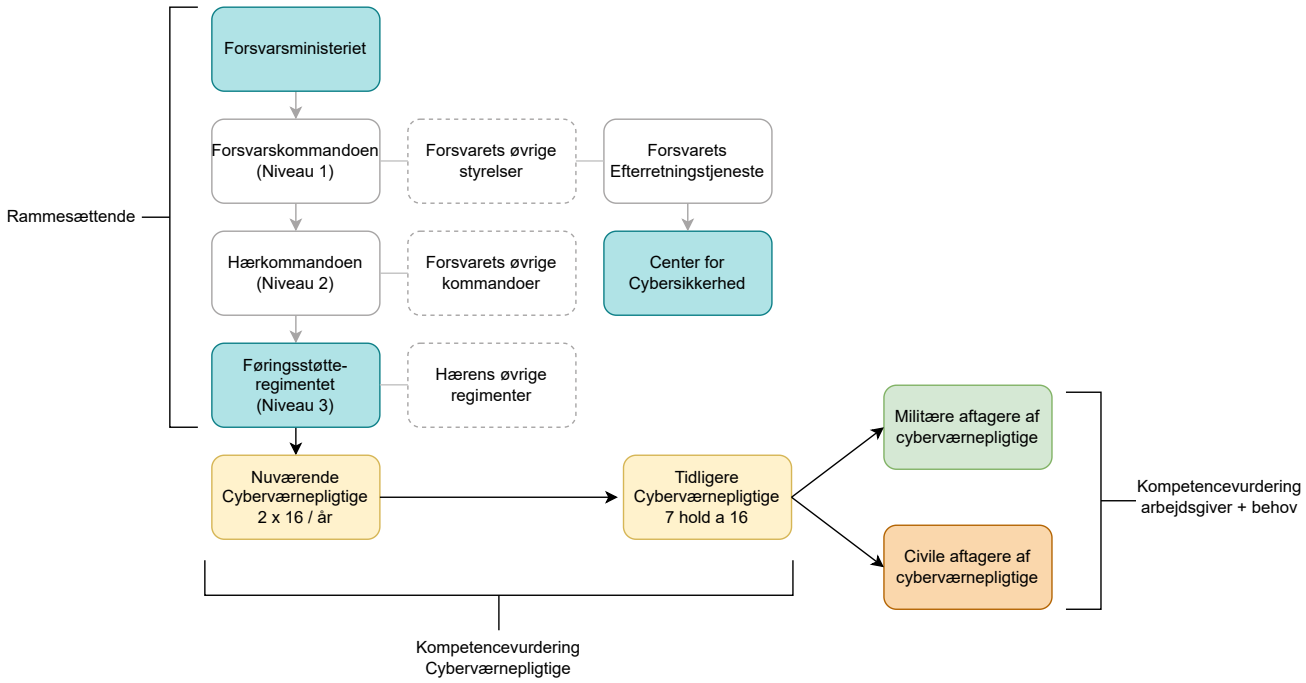
På trods af, at Forsvarets Cyberværnepligt ikke fremgår af hverken national cyber- og informationsstrategi 2018-2023 eller af forligsteksten, italesættes den fra politisk hold til offentligheden fra april 2019. Forsvaret præsenterer cyberværnepligtuddannelsen i november samme år, med holdstart februar 2020. Uddannelsen er henvendt unge der *"vil udvikle deres digitale færdigheder i Forsvaret gennem den nye værnepligt - til gavn for dem selv og for hele Danmark"* (Personalestyrelsen, 2019). Uddannelsen er ikke designet til efterfølgende varig ansættelse i Forsvaret, men er snarere en grunduddannelse indenfor cyber- og IT. Cyberværnepligten oprettes som en 3-årig forsøgsordning, med indledningsvist 32 værnepligtige per år. Særligt motiverede ansøgere, som har gennemført den almindelige 4-måneders værnepligt, samt bestået en optagelsesprøve til Forsvarets dag (Personalestyrelsen, 2019), har mulighed for at påbegynde cyberværnepligtsuddannelsen på 6 måneder
Uddannelsens formål er: *"at styrke Forsvarets og samfundets beskyttelse mod cybertrusler i fred, krise og krig"*, bilag [G3]. Cyberværnepligten bidrager således til både at styrke samfundets og Forsvarets beskyttelse mod trusler fra cyberdomænet. Uddannelsen er, på trods af dens forankring i Forsvaret og financiering under Forsvarsforliget, ikke målrettet efterfølgende jobmuligheder i Forsvaret. Uddannelsen gennemføres ydermere i vekselvirkning mellem intern og ekstern undervisning ved militære og civile samarbejdspartnere, bilag [G3]. Indholdet af uddannelsen indbefatter bl.a. grundlæggende og alsidige elementer indenfor: IT og hardware, netværksteori, servere og services, cyber-viden, samt IT- og netværkssikkerhed, bilag [G3]. Cyberværnepligtige opnår gennem uddannelsen en grundlæggende viden, færdigheder og kompetencer. De godtskrives merit på 7 uger til IT-supporter uddannelsen (til Syddansk Erhvervsskole, bilag [G3]). Desuden modtager deltagere efter endt uddannelse et kompetencekort, der beskriver opnåede kompetencer. Her fremhæves indenfor personlige kompetencer: *samarbejde, disciplin, respekt, ansvar, selvstændighed og fællesskab*. Derudover fremhæves særlige kompetencer som: *"rutineret viden om server, netværk og infrastruktur"*samt *"evnen til at bevare ro og kontrol i pressede situationer"*, bilag [G2]. Efter 3 forsøgsår er cyberværnepligten blevet permanent fra sommeren 2023. Efter de første 6 hold bestående af 80 cyberværnepligtige, er 36 fortsat i job inderfor Forsvarsministeriets område (Forsvaret, 2023b).



Figur 1.1: Overblik over cyberværnepligtens uddannelsesforløb, bilag [G1]

1.2.2 Caseområde

Forsvarsministeriet er et ministerium som alle andre, der bl.a. varetager Forsvarets økonomi og Forsvarsforliget. Ministeriet arbejder på politisk niveau. Under Forsvarsministeriet findes en styrelsesstruktur, hvoraf Forsvarskommandoen blot er en af mange på samme niveau (Niveau 1 myndighed) med selvstændige styrelseschefer (Forsvarsministeriet, 2024b). Forsvarskommandoen indeholder det, der i folkemunde omtales som "Forsvaret", forstået som størstedelen af soldater og enheder, fly, skibe, panser mv. Disse enheder er underlagt 5 forskellige kommandoer på samme niveau (Niveau 2 myndigheder), (f.eks. Hærkommandoen, Søværnskommandoen mv.). Under Hærkommandoen findes forskellige regimenter (Niveau 3 myndigheder), der hver har forskellige specialer, der danner rammen for løsning af Forsvarets opgaver (Forsvaret, 2024b). Et af disse regimenter er Føringsstøtteregimentet hjemhørende i Fredericia (Forsvaret, 2024a). I Føringsstøtteregimentet findes forskellige bataljoner, som varetager forskellige opgaver og har forskellige ansvarsområder. Uddannelse af cyberværnepligtige foregår i 3. CISOPBTN (3. Communications and Informations Operationsstøttebataljon), der bl.a. omfatter: IT- og cybersikkerhed og IT-uddannelser.



Figur 1.2: Overblik over struktur og aktører

Forsvarets struktur og organisation bevirker, at der er en klar og tydelig kommandovej. Det betyder samtidigt, at den vertikale hierarkiske sti er karakteriseret af mange ledelseslag med tilhørende chefer, der varetager forskellige enheder og opgavetyper, som kan konkurrere om samme fokus eller ressourcer. Forsvaret er, som alle andre offentlige forvaltningsinstitutioner, underlagt den parlamentariske styrings- og delegationskæde, forstået på den måde, at Forsvaret må efterleve den til enhver tid siddende Regering. De trækker sin legitimitet fra den regeringsudpegede minister, i Forsvarets ressortområde Forsvarsministeren, som træffer beslutninger med gyldighed for Forsvaret (Christensen, Christiansen, og Ibsen, 2017, s. 57).
Med Forsvarets organisationsstruktur og forhold adresseret, beskrives i næste afsnit de afgrænsninger, som naturligt forekommer, samt afgrænsninger, der er valgt til undersøgelsen.

1.2.3 Afgrænsinger

I dette afsnit beskrives undersøgelsens afgræsninger, hvilket opdeles i valgte afgrænsninger og naturlige afgrænsninger, som forekommer i forbindelse af samarbejde med Forsvaret.

Valgte afgrænsninger

Denne undersøgelse afgrænses hierarkisk til uddannelse af cyberværnepligtige under 3. CISOPBTN ved Føringsstøtteregimentet samt deres efterfølgende virke ved militære eller civile aftagere af disse jf. figur 1.2. Derved afgrænses fra dybdegående undersøgelse af enheder/interessenter i niveau 1-3 myndigheder samt

Forsvarsministeriet. Enheder/interessenter i disse lag bruges til at rammesætte problemområdet.

Undersøgelsen afgrænses ydermere fra at omhandle selve indholdet af cyberværnepligtsuddannelsen. Det vil sige sammensætning af kurser og indholdet deri. Dette skyldes, at uddannelsesmaterialet til dels er klassificeret, og at flere af kurserne afholdes af udefrakommende konsulenter, hvor uddannelsesofficererne ved FSR kun har overordnet planlægningsansvar. Dermed afgrænses undersøgelsen fra, om de enkelte læringsmål opfyldes. Ligeledes afgrænses undersøgelsen fra at evaluere, om uddannelsens formål opfyldes, da selve formålsformuleringen er generel og bredt formuleret, hvilket gør evt. målopfyldelsesevaluering meningsløst.

Naturlige afgrænsninger

Evaluering af hvorvidt den politiske målsætning opfyldes af cyberværnepligten foretages ikke, eftersom antallet af beslutningsled fra Forsvarsministeriet til aftagerne af de cyberværnepligtige, vurderes for omfangsrigt til at en sådan evaluering kan ske med nøjagtighed. Denne pointe underbygges yderligere af, at dokumenter indeholdende målsætning, budget mv. er klassificerede. Grundet manglende formålsbeskrivelser og budgetter, er det heller ikke muligt at evaluere, hvorvidt cyberværnepligten fra et økonomisk perspektiv er fordelagtigt, eller et bedre alternativ end andre uddannelser.

1.3 Undersøgelsesdesign

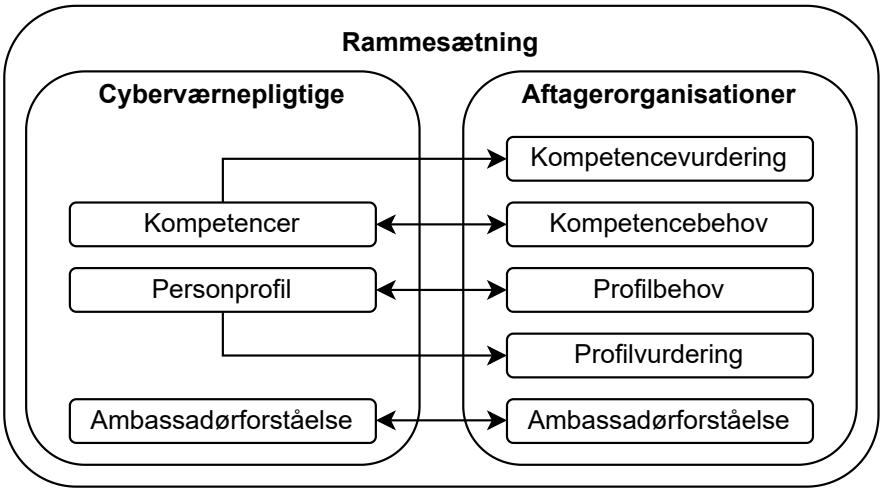
På baggrund af undersøgelsens caseområde og afgrænsninger, har dette afsnit til formål at beskrive, hvordan problemformuleringen besvares, samt hvordan undersøgelsen struktureres. Problemformuleringen besvares igennem en syntetisering af besvarelserne af de tre underspørgsmål, hvortil diskussionspunkter inddrages. De tre underspørgsmål besvares individuelt ud fra følgende beskrivelser:

- **Underspørgsmål 1** omhandler vurdering af de cyberværnepligtiges kompetencer og profil fra aftagernes perspektiv. Derudover vurderes det fra aftagernes perspektiv, hvorvidt de cyberværnepligtiges kompetencer og profil er passende til de respektive aftagerorganisationer.
- **Underspørgsmål 2** skelner mellem de cyberværnepligtiges kompetencer og profil, og de kompetence- og profilbehov, som aftagerorganisationerne har. De cyberværnepligtiges kompetencer og profil afdækkes gennem en kombination af selvevaluering af hhv. nuværende og tidligere cyberværnepligtige, samt aftagernes vurdering af de cyberværnepligtiges kompetencer og profil fra underspørgsmål 1. Aftagerorganisationernes kompetence- og profilbehov afdækkes gennem ledelsen fra militære og civilie organisationer, som har været med til at ansætte de cyberværnepligtige. Slutteligt sammenholdes de cyberværnepligtiges kompetencer og profil med aftagerorganisationernes kompetence- og profilbehov m.h.p. at fremhæve evt. uoverensstemmelser herimellem.

- **Underspørgsmål 3** undersøger hvordan rollen som ambassadør for god IT-sikkerhed manifesteres hos hhv. de nuværende og tidligere cyberværnepligtige, samt militære og civile aftagere. Igen sammenholdes disse perspektiver m.h.p. at fremhæve evt. uoverensstemmelser herimellem.

- **Rammesætningen** undersøges m.h.p. at nuancere cyberværnepligtens formål fra flere hierarkiske niveauer. Denne nuancering inddrages i analysen og diskussionen til at sætte besvarelserne af underspørgsmålene i perspektiv. Rammesætningen undersøges gennem Forsvarsministeriet, Føringsstøtteregimentet og CFCS.

Ovenstående beskrivelse af hvordan underspørgsmålene besvares, indeholder forskellige perspektiver, hvilke ses illustreret i figur 1.3.

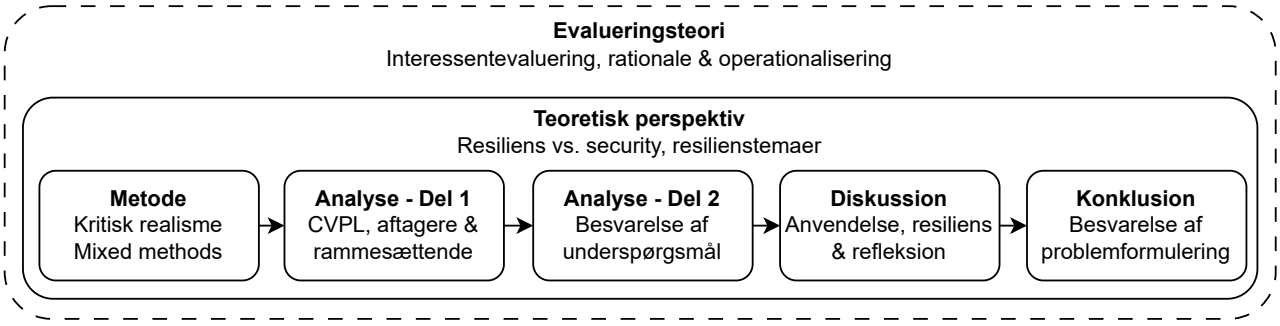


Figur 1.3: Undersøgelsesdesign til brugerevaluering og besvarelse af problemformulering

I figuren ses hvilke undersøgelsesområder, der tilhører den specifikke interessentgruppe, hvor f.eks. kompetencer, personprofil og ambassadørforståelse undersøges igennem de cyberværnepligtige. Som tidligere nævnt, er cyberværnepligten endnu ikke evalueret fra et brugerperspektiv. I undersøgelsesdesignet anses aftagerorganisationerne som værende brugere af cyberværnepligten. Undersøgelsen retter derfor fokus mod en brugerevaluering af cyberværnepligten centreret omkring aftagerorganisationerne. Undersøgelsesdesignet danner udgangspunkt for undersøgelsens opbygning og struktur, hvilket beskrives i næste afsnit.

1.3.1 Undersøgelsesstruktur

Undersøgelsen struktureres som vist i figur 1.4. Figuren inddrages som en del af metateksten i de respektive kapitler, hvor det enkelte kapitel fremhæves ved at farve de øvrige grå. Dette har til hensigt at danne overblik og skabe transparens igennem undersøgelsen. I figuren udgør elementerne fra *Metode* til *Konklusion* selve hovedundersøgelsen. *Analyse - Del 1* og *Analyse - Del 2* tager udgangspunkt i figur 1.3, hvor del 1 struktureres efter de tre interessentgrupper, og del 2 struktureres ud fra underspørgsmålene. Det teoretiske perspektiv i kapitel 2 er gennemgående for hele hovedundersøgelsen, og vil derfor også fremgå markeret, når elementer i hovedundersøgelsen beskrives. Evalueringsteorien i kapitel 4 danner rammerne for undersøgelsen, men indgår ikke direkte i analysen, og ses derfor fremtrædende med en stiplet linje.

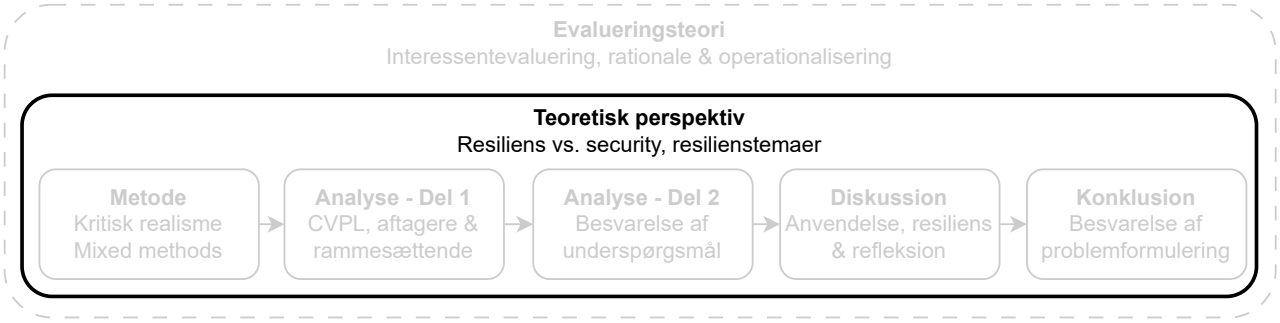


Figur 1.4: Undersøgelsesstruktur

Kapitel 2

Teoretisk perspektiv

Dette kapitel har til formål at fremføre det teoretiske perspektiv, som anvendes igennem undersøgelsen. I efteråret 2023 gennemførte specialegruppen et litteraturstudie med følgende ordlyd: *Hvilke faktorer indenfor litteraturen er afgørende for ledelse af cyberresiliens?* Undersøgelsen indtager et akademisk perspektiv på fænomenet, og er en kondensering og syntesering af den videnskabelige litteratur på området (Se bilag [K1]). Afsnittet herunder vil udfolde litteraturstudiets metodiske tilgang samt de mest relevante fund. Som vist i figur 2.1, er det teoretiske perspektiv på cyberresiliens styrende for: hvordan undersøgelsen udformes; hvordan empirien indsamles og behandles; og dertil problemformuleringen besvares. Dette afsnit vil fremlægge den metodiske fremgangsmåde og fund for det teoretiske perspektiv gennem visuelle præsentationer, og henvise til bilag for fuld indsigt i mellemliggende analyser.



Figur 2.1: Teoretisk perspektiv i undersøgelsen

2.1 Metode - Teoretisk perspektiv

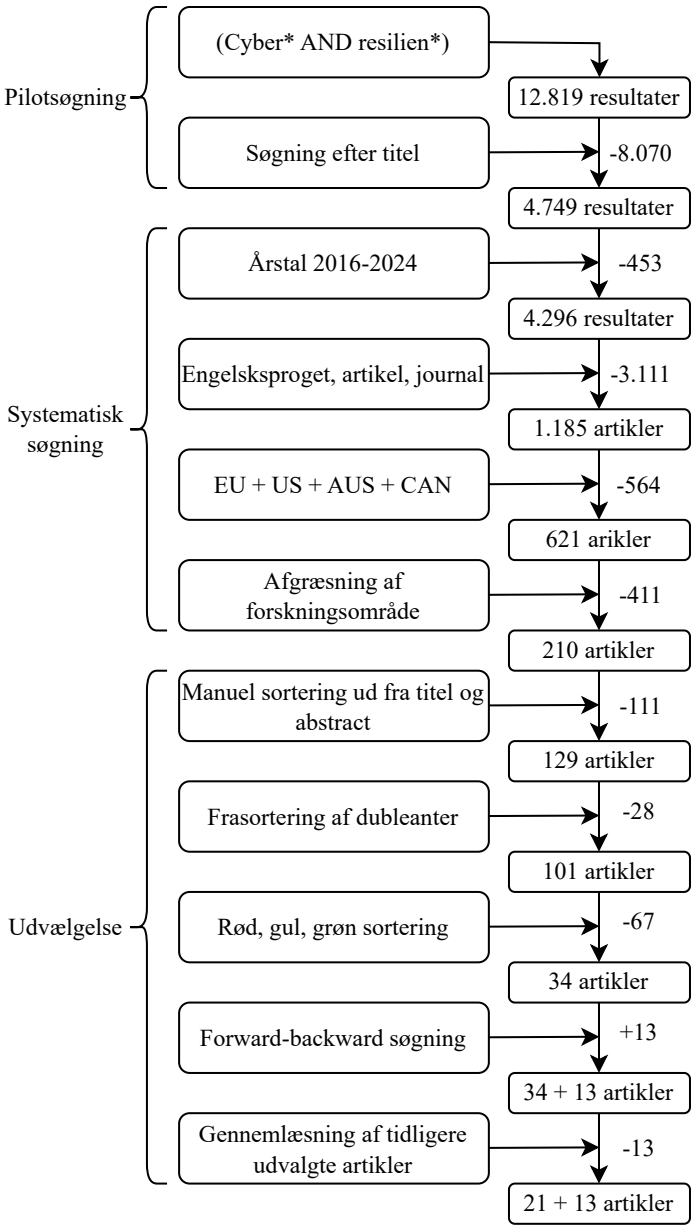
Litteraturstudiet blev gennemført med afsæt i *National Institute of Standards and Technology's (NIST)* definition på cyberresiliens:

> *The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."(Ross, Pillitteri, og Dempsey, 2022, s. 38)*

NIST supplerer dette med underpunktet: *"Cyber resiliency can be a property of a system, network, service, system-of-systems, mission or business function, organization, critical infrastructure sector or sub-sector, region, or nation."* (Ross et al., 2022, s. 38). I det ovenstående supplement fremgår et iboende fokus mod organisationen og dens mission, strategi og funktion. En naturlig forlængelse af dette er, at litteraturstudiet afgrænses til en undersøgelse på organisationsniveau. Litteraturstudiet har ligeledes et ledelsesmæssigt fokus fremfor et teknisk perspektiv, da cyberresiliensbegrebet favner bredere end blot tekniske foranstaltninger.

2.1.1 Metodisk tilgang

Litteraturstudiets design er baseret på *Wolksvinkel et al.* femtrinsstruktur. Det bygger på et design, der opstiller in- og eksklusionskriterier, indeholder flere iterationer af pilotsøgning (4749 artikler) inden endelig og systematisk litteratursøgning blev gennemført (210 artikler). Herefter foregår en udvælgelsesproces og gennemlæsningsproces, der medførte en slutvolumen på 33 peer-reviewed, videnskabelige artikler publiceret i anerkendte engelsksprogede journaler. Figur 2.2 er en visuel repræsentation af metoden. De udvalgte artikler er herefter kodet efter induktive principper i form af åben-, aksial- og selektiv kodning, da fempunktsstrukturen har afsæt i grounded theory, bilag [K1].



Figur 2.2: Visualisering af søgeproces (Bilag [K1])

Fund: På baggrund af den metodisk fremgangsmåde, identificeredes fire hovedområder med tilhørende underkategorier. De fire områder er: *aktører, ledelse, organisatorisk resiliens og teknologi*. De fire kategorier indeholder en række tilhørende underkategorier, hvoraf de mest dominante og fremtrædende udfoldes og diskuteres i litteraturstudiet, og de sekundære kategorier optræder i studiets tilhørende bilag [K1]. Nedenstående tabel giver overblik over hovedtemaer samt primære og sekundære underkategorier.

Hovedtema	Primær kategori	Sekundær kategori
Aktører	Medarbejdere	Ansvarsfordeling
	Modstandere og angreb	Eksterne aktører
		Supply chain
Ledelse	Ledelse af resiliens	IT-lederens rolle
	Policy	Topledelse
	Governance	Processer
	Kapabiliteter	Strategi
	Kommunikation	Compliance
	Risk management	
Organisatorisk resiliens	Frameworks	Faser og tid
	Awarness og kultur	Modenhede
	Organisatorisk læring	Interne faktorer
	Organisatorisk resiliens	Alignment
		Evaluering af resiliens
		Forandringsledelse
		Testing
Teknologi	Data	AI
	Teknologisk best practise	IoT

Tabel 2.1: Overblik over temaer og kategorier

Et centralt fund ved litteraturstudiet er, at på trods af fokus har været på hvilke faktorer litteraturen fremhæver som afgørende for ledelse af cyberresiliens, bruges begrebet cyberresiliens ofte synonymt med begrebet *cybersecurity*. I andre tilfælde er der overlap mellem de to begreber, og de er en del af hinanden. På trods af, at begrebet *cyberresiliens* var i fokus, er der på tværs af den undersøgte videnskabelige litteratur konsensus om, at *cybersecurity* kan ses som en del af det at skabe *cyberresiliens*.

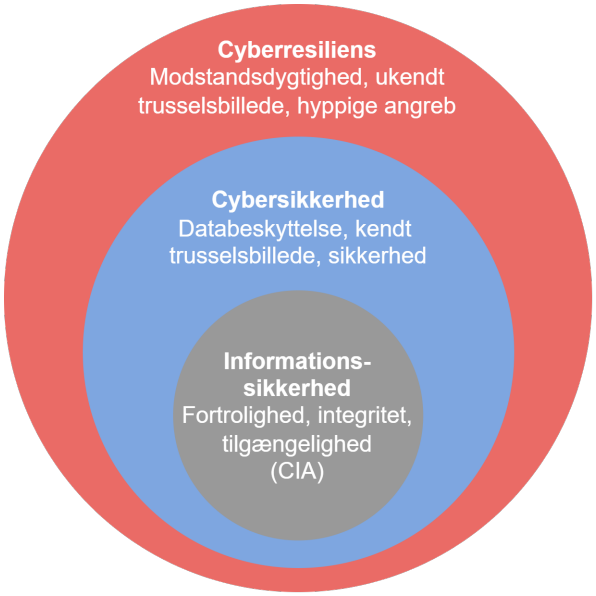
2.2 Cyberresiliens vs. cybersecurity

Ved at kondensere og sortere den undersøgte litteratur jf. bilag [K1], er det muligt at forstå *cybersecurity* og *cyberresiliens* gennem følgende definitioner, der sidenhen vil finde anvendelse i undersøgelsen. Definitionerne bygger på syntese af nuværende perspektiver på begreberne, der fremgår af den videnskabelige litteratur:

Cybersecurity: *Cybersecurity defineres som beskyttelse, såvel som bevarelse af begreberne confidentiality, integrity og avalibility (CIA) i informationssystemer, hvor mennesker og software kommunikerer med brug af computere og forbundne systemer på internettet. Cybersecurity omfatter beskyttelse af systemer mod uautoriseret adgang, mod angreb der kan føre til datatab, forstyrrelse eller i værste fald ødelæggelse af systemer.*

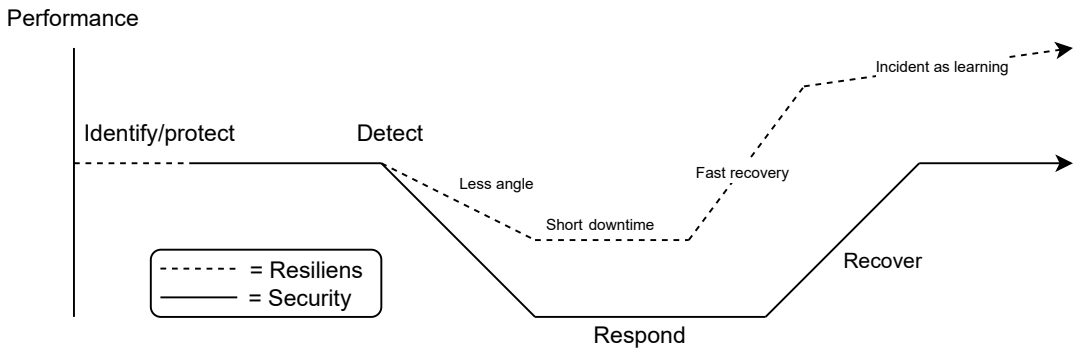
Cyberresiliens: *Cyberresiliens defineres som en organisations evne til at fortsætte sine kerneformål og bevare sin integritet under cyberhændelser. Cyberresiliens er evnen til at forberede sig på, modstå, reagere og komme sig efter en cyberhændelse. Cyberresiliens er multifacetteret og indbefatter udover evnen til at beskytte sig også kapabilitet til at opretholde, hurtigt genoprette drift og funktionalitet, sikre kontinuerlig drift og beskytte kritiske data under og efter cyberhændelser.*

Definitionerne indeholder de mest fundamentale aspekter ved begge begreber. Det fremgår, at cybersecurity er mest fokuseret på proaktiv beskyttelse samt opretholdelse af *CIA*, mens cyberresiliens indtager et bredere og mere holistisk perspektiv. Dette inkluderer en adaptiv strategi hvor tilpasning, læring og genrejsning er i fokus. Det kan oversættes til, som beskrevet af Baikloy, Praneetpolgrang, og Jirawichitchai (2020, s. 917), at CIA er en del af cybersecurity, og at cybersecurity er en del af cyberresiliens, hvilket er visualiseret i figur 2.3. Overlappet mellem begreberne, og integration af cybersecurity som en del af cyberresiliens, medfører sandsynligvis en del af forklaringen på, at litteraturen ofte anvender begreberne synonymt.



Figur 2.3: Cybersikkerhed vs. cyberresiliens
(Baikloy et al., 2020)

Cybersecurity har et kortere og mere snævert virke, der også typisk foregår på et mere teknisk niveau, mens cyberresiliens typisk foregår i et bredere perspektiv og udføres på et mere organisatorisk og ledelsesmæssigt niveau. Det er centralt at bemærke, at cyberresiliens indeholder et lærende element, hvor organisationen udvikler sig og bliver bedre over tid og/eller kommer styrket ud af et cyberhændelsesforløb.
De to forskellige begreber kan forstås gennem nedenstående figur 2.4:



Figur 2.4: Cybersikkerhed vs. cyberresiliens

2.3 Temaer i det teoretiske perspektiv

Dette afsnit skitserer de temaer, som anvendes fra det teoretiske perspektiv (bilag [K1]) til brug i analysen. Fravalgte temaer kan findes i bilag [J1].

Opsummering af aktører

Tabel 2.2 fremhæver udvalgte pointer fra litteraturstudiet indenfor temaet *aktører*. For temaet aktører kan det opsummerende siges, at fokus er på det kollektive ansvar i opbygningen af cyberresiliens. Herunder er fokus i høj grad på medarbejdere, uddannelse af sine medarbejdere, og samarbejde på tværs af organisationens økosystem. Dette perspektiv skal forstås i konteksten af trusler, særligt insider-trusler (Se bilag [K1]).

Aktører	**Vigtige pointer**	**Reference**
Medarbejdere	- Intern rollefordeling	[16, 11, 27]
	- Fælles forståelse for cyberresiliens	[24, 22, 38, 16, 11]
	- Træning og uddannelse	[24, 22, 12, 35, 36, 16, 25, 13]
Modstandere og angreb	- Insider threats	[32, 35, 36, 13]
	- Cyber threat intelligence	[36, 19, 34]
	- Ledelsesmæssige cyber-værktøjer	[25, 21, 18]
Ansvarsfordeling	- Holistisk ansvar	[21, 9, 13, 37, 14, 34]
	- Skarpe rammer for eksterne partneres ansvar	[21, 9, 13, 37, 14, 34]
Eksterne aktører	- Gensidig forståelse	[12, 16, 19, 9, 21, 13, 14]
	- SME anbefales ekstern hjælp	[12, 16, 19, 9, 21, 13, 14]

Tabel 2.2: Vigtige pointer fra aktør-afsnittet

Opsummering af ledelse

Tabel 2.3 fremhæver udvalgte pointer fra litteraturstudiet indenfor temaet *ledelse*. For temaet ledelse kan det opsummerende siges, at fokus er på topledelse, strategisk ledelse og evnen til at anvende ledelsesbegreber, som governance, risk & compliance, hvilket står overfor mere bottum-up begreber, som kommunikation, kapabiliteter og uddeligering af ansvar. Derudover skal ledelse af cyberresiliens baseres på anerkendte frameworks (Se bilag [K1]).

Ledelse	**Vigtige pointer**	**Reference**
Ledelse af resiliens	- Support fra top-ledelse er essentiel - Pro-aktiv kommunikation - Risk-management og frameworks	[22, 28, 9, 37] [12, 28, 9, 18, 13, 37, 14] [12, 28, 27, 18, 22, 35, 9, 13, 37, 14, 34]
Governance	- Governance er vigtigt for topledelsesopbakning - Governance er supporterende for brug af standarder og frameworks, og relateret til policy	[38, 12, 20, 28, 37] [38, 28, 37, 13, 20, 28]
Kommunikation	- Kommunikation er centralt for opbygning af cyberresiliens - Kommunikation er særligt vigtigt ved læring fra angreb under recoveryfasen	[22, 20, 3] [12, 35, 3]
Risk management	- Risk-management er et vigtigt ledelsesbegreb. - Risk-management bør i cyberresiliens betragtes hollistisk og inkludere menneskelige aspekter	[32, 36, 20, 19 [36, 19, 10]
Strategi	- Forretningsstrategi skal lede cyberstrategien	[20, 10]
Compliance	- Compliance er relateret til standarder og frameworks - Compliance relateres til organisationens kultur	[39] [39]

Tabel 2.3: Vigtige pointer fra ledelsesafsnittet

Opsummering af organisatorisk

Tabel 2.4 fremhæver udvalgte pointer fra litteraturstudiet indenfor temaet *organisatorisk resiliens*. For temaet organisatorisk resiliens kan det opsummerende siges, at fokus er på benyttelsen af standardiserede frameworks, samt aktivt at benytte de indbyggede faser før, under og efter et angreb. Organisationer kan udvikle sig, ved særligt at lærer af angreb, både under og efter. Som tilføjelse hertil, kan træning og kultur spille en stor rolle, dog eksisterer der ikke konsensus om en tilgang til dette (Se bilag [K1]).

Organisatorisk	**Vigtige pointer**	**Reference**
Frameworks	- Standarder som NIST dominerer	[7, 38, 5, 19, 10, 21, 18, 13]
	- Stor kompleksitet kræver god ledelse	[5, 14, 24, 38, 23, 21, 37]
	- Overensstemmelse på tværs af organisationer	[13, 14]
	- Ressourceallokering	[5, 8, 14]
	- Stor udfordring for SMV'er	[5, 8, 14, 25]
Awareness og kultur	- Træning og uddannelse til kulturændring	[36, 20, 39, 28, 3, 25, 37]
	- Top-down kommunikation er essentiel	[20, 39, 28, 3, 25, 37]
	- Leders rolle: at forstå ansatte	[20, 36, 39, 3, 37]
	- Ledelsens rolle: at agere champions	[19, 39]
	- Forandringsledelse og gamification	[36, 20, 39, 3, 37]
Organisatorisk læring	- To-vejs kommunikation og feedback.	[24, 12]
	- Læring, adaption og evaluering	[38, 35, 36, 25, 8, 13, 37, 14]
	- Ledelsen bliver proaktive	[38, 35, 36, 25, 8, 13, 37, 14]
Organisatorisk resiliens	- Overblik fra ledelsen ift. sårbarheder, træning og eksterne partnere	[2, 37]
	- Ressourceallokering	[2, 25]
	- Rollefordeling og sikkerhedskultur	[21, 37]
	- Cyberresiliens som forretningsstrategi	[12, 8, 14]
	- Ledelsmæssig forståelse for at være Pro-aktiv og at kunne identificere og mitigere trusler	[2]
Modenhed	- Plan management.	[4]
	- Kommunikation, evaluering og læring	[25]

Tabel 2.4: Vigtigste pointer for organisatorisk resiliens

Opsummering af Teknologi

Tabel 2.5 fremhæver udvalgte pointer fra litteraturstudiet indenfor temaet *teknologi*. For temaet teknologi kan det opsummerende siges, at fokus er på data, både som genstand og som værktøj, teknologisk best practice, og teknologier, der er med til at sikre cyberresiliens i organisationer. Teknologi indgår ligeledes som en del af organisationens struktur, samt er en del af ledelsens værktøjkasse (Se bilag [K1]).

Teknologi	**Vigtige pointer**	**Reference**
Data	- Data som beskyttelseselement med fokus på databeskyttelse.	[35, 36, 16, 11, 20, 19, 28]
	- Data som kilde til forbedring af cyberresiliens.	[16, 36, 20, 28]
Teknologisk best practice	- Teknologi som præventiv foranstaltning.	[35, 11, 25, 21, 9]
	- Teknologiske tiltag er de vigtigste for at opnå cyberresiliens.	[35, 11, 25, 21, 9, 10]

Tabel 2.5: Centrale pointer fra teknologiafsnittet

2.4 Operationalisering af teoretisk perspektiv

Med afsæt i litteraturstudiets udfoldelse af temaerne; *aktører, ledelse, organisatorisk resiliens* og *teknologi* og forståelse for litteraturens syn på cyberresiliens og cybersecurity, vil undersøgelsen anvende dette som teoretisk perspektiv i analyse del 2 i kapitel 6 og diskussion i kapitel 7. Temaerne vil fungere som teoretisk grundlag for, at analysere forholdet mellem aftagerorganisationerne, de tidligere og nuværende cyberværnepligtige samt inddragelse af de rammesættende interessenter. Formålet er, at give undersøgelsen et teoretisk perspektiv hvorigennem cyberresiliens forståes, samt diskuteres i kapitel 7 *(Diskussion)*. Det teoretiske perspektiv har, udover sin anvendelighed i analysen, været afsæt for den metodiske tilgang i afsnit 3 *(Metode)*.

Kapitel 3

Metode

I dette afsnit udfoldes de metodiske greb som anvendes til at besvare problemformuleringen og underspørgsmålene. Hertil præsenteres indledningsvist undersøgelsens videnskabsteoretiske positionering; *kritisk realisme*. Metodeafsnittets hensigt er at udfolde både den videnskabelige systematik, undersøgelsens betingelser, samt de metodiske værktøjer, som benyttes med formålet om at kunne evaluere de cyberværnepligtige m.h.p. at besvare undersøgelsens underspørgsmål. Som vist i figur 3.1, er de metodiske rammer gennegående for de øvrige afsnit, men er herudover også dikterende for valget af evalueringstilgang, som beskrives i afsnit 4.

Figur 3.1: Metode i undersøgelsen

3.1 Videnskabsteori

Afsnittet har til formål at udfolde specialets videnskabsteoretiske ståsted. Hensigten er, at læseren gøres bevidst om hvordan verden og viden anskues, og dermed også de metoder og slutninger denne position inkluderer. Det gøres ved at udfolde ontologi, epistemologi, metodologi, slutningsform og kvalitetskriterier.

3.1.1 Positionering

Undersøgelsen positionerer sig videnskabsteoretisk ved *Kritisk Realisme*. Kritisk realisme giver en position, hvor den videnskabsteoretiske dualisme ikke er et valg mellem to muligheder, men en kombination af disse (Ingemann, 2017, s. 88). Den videnskabsteoretiske position opstår på baggrund af samhørig konsensus og verdenssyn efter længeregående uddannelse indenfor samfundsvidenskab, hvor dualisme ofte er en nødvendighed. Specialets undersøgelsesområde og problemfelt falder indenfor en samfundsvidenskabelig problemstilling, og derfor en naturlig forlængelse af vores videnskabsteoretiske ståsted.

Ontologi

Ontologisk set, er virkeligheden for os noget der findes og kan tilgås. Virkeligheden eksisterer uafhængigt af os, og som andre også kan opnå adgang til. Vi opfatter virkeligheden som noget komplekst, og noget der manifesterer sig gennem forskellige strukturer. Disse metoder kræver forskellige tilgange, for at tilgå de strukturer og lag der ikke umiddelbart er observerbare; de lag vi kun kan forstå gennem tolkning, sandsynliggørelse og teoretisering. Når virkeligheden opfattes som værende kompleks, optræder flere forklaringer af samme fænomen, som alle kan forstås på forskellige måder. Det anerkendes derved, at der er indbyggede afhængigheder, og at universelle sandheder derfor ikke forekommer entydigt, og er derfor heller ikke formålet med undersøgelsen. Knytningen til kontekst medfører naturligt at undersøgelsens fund ikke nødvendigvis kan applikeres til andre områder, da konteksten for undersøgelsen har betydning for den oplevede virkelighed.

Epistemologi

I undersøgelser med afsæt i kritisk realisme, tilgås verden gennem forskellige forståelseslag. De øverste lag er tilgængelige via observation, data, tendenser mv, mens det dybeste lag kun kan tilgås og forstås gennem tænkning, hvoraf teori spiller en afgørende rolle (Ingemann, 2017). Undersøgelsesdesignet er tiltænkt for at kunne indhente viden på tværs af disse lag. I praksis betyder det forskellige metoder, der spiller forskellige roller alt efter, hvor de anvendes. Nedenstående figur 3.2 viser sammenhæng mellem kritisk realismes tre strata (Ingemann, 2017, s. 93) og opertionalisering af undersøgelsens anvendte metoder. Teori anvendes aktivt til at forstå de dybereliggende strukturer, samt kontekst og afhængigheder.

EMPIRISK STRATUM

Data, målinger

Operationalisering: Interviews, klyngeinterview, observationsstudie, spørgeskemaer mv.

- -

FAKTUELT STRATUM

Hændelser, tendenser

Operationalisering: Behandlet/analyseret empiri

DYBE STRATUM

Kausale mekanismer, magtstrukturer, institutionelle forhold

Operationalisering: Teoretisk perspektiv

Figur 3.2: Figur over de tre strata baseret på Jespersen
(Ingemann, 2017, s. 93)

Metodologi og slutningsform

Virkeligheden anskues som værende tilgængelig både via induktiv observation og deduktiv refleksion. Vi anvender tilgange og metoder, der tilgodeser begge positioner alt efter hvilke lag, der søges afdækket. De øvre lag tilgås gennem induktive metoder, mens de dybe lag ikke umiddelbart lader sig observere, og tilgås derfor kun via refleksion med teori som afgørende rettesnor (Ingemann, 2017). Empiri og teori betragtes som lige komponenter og hinandens forudsætning, der anvendes på forskellige niveauer. Kombinationen af de to tilgange, samt erkendelsen af, at virkeligheden er kompleks og kontekstafhængig, medfører at slutningsformen abduktion vil anvendes. I erkendelse af, at sammenhænge aldrig fuldt afdækkes på baggrund af ontologiske og epistemologiske erkendelse, besvares problemformuleringen i stedet gennem sammensmeltning af teori og empiri, hvortil abduktion findes særligt anvendelig som slutningsform.

Kvalitetskriterier

I forlængelse af metodologi og slutningsformen, samt erkendelsen af, at verden er kompleks og kontekstafhængig, vurderes kvalitet i undersøgelsen særligt ud fra to primære kvalitetskriterier. De to kriterier udvælges for at kunne vurdere kvalitet gennemgående og konsistent i undersøgelsen.

Transparens som kvalitetskriterie: Første kvalitetskriterie er transparens. I erkendelsen af, at der er strukturer, mekanismer og uobserverbare fænomener, der har betydning for kontekst (Ingemann, 2017), er transparens og gennemsigtighed for læseren et kriterie, der ses som værende vigtigt for de rationaler og slutninger der foretages. Det vil i praksis udføres med formål om at præcist kunne henvise og dokumentere metodologi og processer fra faktuelle observationer til abstraktioner. Særligt under behandling af kvalitativ

data, samt abstraktion ved hjælp af teori, findes det særligt nødvendigt med en høj grad af transparens.

Metodisk selvrefleksion som kvalitetskriterie: I det kritisk realistiske paradigme eksisterer multikausale sammenhænge, hvorfor det ikke giver mening at søge efter universelle lovmæssigheder (Ingemann, 2017, s. 100). Derfor vil der naturligt være forskellige metoder til af afdække verden, der alle sammen vil være gangbare. Derfor anses metodisk selvrefleksion som et kvalitetskriterie, der skal tilsikre velovervejede og dokumenterede metodevalg, som kan diskuteres og reflekteres over med dets indbyggede fordele og ulemper. Den metodiske selvrefleksion knytter sig naturligt til både de kvalitative og kvantitaive tilgange og er gældende i alle afsnit.

3.2 Interessentoverblik

Dette afsnit har til formål at danne overblik over undersøgelsens interessenter, samt de metodiske tilgange til udvælgelse af disse. Grundet undersøgelsens evaluerende natur, er udvælgelsen og overblikket over interessenter essentielt, særligt som forudgående stadie til evalueringens foretagelse jf. figur 3.3. Dette betyder, at sampling er tillagt en særlig betydning, både for hvordan interessenterne er udvalgt og prioriteret, men også med hvilke metodiske værktøjer som benyttes. Interessenterne er differentieret i interessentoverblikket jf. afsnit 1.3, hvor de tre primære interessentgrupper for cyberværnepligten udfoldes: rammesættende enheder, de cyberværnepligtige selv, og aftagerne.

3.2.1 Sampling

Der anvendes forskellige tilgange til sampling for hhv. kvalitativ og kvantitativ metoder, som udfoldes herunder. Afsnittet har til hensigt at skabe gennemsigtighed i hvorledes sampling er gennemført.

Sampling til kvalitative metoder

Sampling til undersøgelse med kvalitative metoder er foregået i tre forskellige trin, der hver har til hensigt at opnå de relevante respondenter indenfor undersøgelsesfeltet, uden samtidigt at kompromittere undersøgelsens integritet eller tillid til samarbejdspartner.

Purposive sampling er anvendt som primær metode til den kvalitative del, og den har til hensigt at sikre at de undersøgte er relevante i forhold til undersøgelsens case fremfor statistisk repræsentative. Purposive sampling anvendes for at opnå så rige og dybe informationer som muligt i forhold til besvarelse af problemformuleringen (Bryman, Clark, Sloan, og Foster, 2021, s. 378). Det betyder at de interviewede personer har direkte relevans i forhold til denne og dens underspørgsmål enten som aftager af cyberværnepligtige eller som rammesættende myndighed.

Snowball sampling er anvendt som metode til at udvide mængden af relevante informanter på baggrund af anbefaling af andre (Bryman et al., 2021, s. 385-386). Metoden er anvendt til både kvantitative undersøgelser og kvalitative interviews. Metoden er ifølge Bryman et al. (2021, s. 385) logisk knyttet kvalitative metoder, men vi finder anvendelsen relevant, da casens problemfelt har en naturlig indbygget sensitivitet overfor datadeling. Snowball-metoden er derfor velegnet, da den bygger på udvidelse af eksisterende netværksrelationer, hvori tillid allerede er opbygget. Ligeledes er kontakt til respondenter opnået gennem snowball-metoden fremfor direkte henvendelse til sensitive aftagere hvor fortrolighed er en dyd.

Criterion sampling er anvendt som metode til udvælgelse af aftagere af cyberværnepligtige. Criterion metoden tilskriver, at der opstilles kriterier til respondenter for deltagelse i undersøgelsen for at få så relevante oplysninger som muligt i relation til undersøgelsesspørgsmål (Bryman et al., 2021, s. 379). Metoden finder anvendelse for at undersøge så tæt på cyberværnepligtens output som muligt. Der er opstillet følgende kriterier for militære og civile aftagere af cyberværnepligtige:

1. De skal være første ordens aftagere (direkte efter cyberværnepligt)
2. De skal bestride en lederstilling eller være ansættelsesansvarlig ift. cyberværnepligtige
3. De skal have et job indenfor eller relateret til cyberområdet

Sampling til kvantitative metoder

Sampling til brug i de kvantitative metoder er foregået af forskellige trin, der alle ligger i relation til non-probability sampling, hvis formål ikke er at kunne generalisere på tværs af population (Bryman et al., 2021, s. 176). Non-probability sampling er en anerkendt metode indenfor socialvidenskaben, og kan skabe næsten ligeså præcise resultater som probability-sampling (Bryman et al., 2021, s. 176).

Convenience-sampling hvor de "tilgængelige"respondenter undersøges (Bryman et al., 2021, s. 176), er anvendt ved "nuværende cyberværnepligtige". Metoden er særligt anvendelig, hvor der ønskes adgang til en population, der er svær at opnå adgang til (Bryman et al., 2021, s. 176-177), hvilket er tilfældet for kategorien "nuværende cyberværnepligtige", da de ikke er registrede i tilgængelige netværk eller databaser og kun kan tilgås via case-samarbejdspartneren FSR. Metoden kan kritiseres for den er med høj sandsynlighed ikke er repræsentativ (Bryman et al., 2021, s. 176). Dette argument findes dog ikke relevant i denne undersøgelse, da besvarelsesprocenten af "nuværende cyberværnepligtige"er tæt på 100 procent af den samlede population.

Snowball-sampling relateres til convenience-sampling og metoden anvendes til at opnå adgang til respondenter via deres forbindelser (Bryman et al., 2021, s. 177+383-385). Metoden er anvendt til at opnå adgang til kategorien "tidligere cyberværnepligtige"og "aftagere af cyberværnepligtige". Metoden vil ikke meføre en repræsentativ population og vil være påvirket af non-responders (Bryman et al., 2021, s. 181-183). En stor del

af "Tidligere cyberværnepligtige"er medlem af en frivillig forening og via den er der opnået adgang til dens medlemmer. Af 112 uddannede cyberværnepligtige, er der ca. 70 medlemmer af foreningen, hvoraf vi har en besvarelsesandel på 41 hvilket udgør 59% procent af foreningens medlemmer. Ligeledes er snowball-sampling anvendt til at opnå kontakt til aftagere af cyberværnepligtige. Metoden findes her særligt relevant, da der ikke findes struktureret overblik over, hvor tidligere cyberværnepligtige har fået job. Metoden kompromitterer ikke ansatte eller undersøgernes integritet, da det foregår via kendte forbindelser. For populationen "aftagere af cyberværnepligtige"findes der 15 respondenter, der totalt har aftaget 27% af den totale mængde cyberværnepligtige.

Non-response i non-probability metoder medfører, at der er en del den samlede population, der ikke ønsker at deltage og at det skævvrider de indsamlede data (Bryman et al., 2021, s. 182). For undersøgelsen vurderes der ikke at være en antalsmæssig problemstilling i relation til non-response, men i stedet vurderes to dele særligt manglende i undersøgelsen. En andel arbejder i klassificerede afdelinger med høj grad af diskretion og anonymitet. Disse vurderes særligt knyttet under Forsvarsministeriets myndighedsområde, og både cyberværnepligtige og deres aftagere optræder i denne gruppe. Ydermere er en del af "tidligere cyberværnepligtige"ikke-interesseret i den frivillige forening eller dens kanaler og er derfor utilgængelige. Det anerkendes, at der er en mindre gruppe, der bevidst ikke søger relation til cyberværnepligten. Antalsmæssigt vurderes størrelsen lille.

3.2.2 Interessenter

Dette afsnit har til formål at danne overblik over undersøgelsens interessenter, samt hvilke specifikke undersøgelsesmetoder der er anvendt til at undersøge den enkelte interessent. Interessenterne er segmenteret jf. undersøgelsesdesignet i afsnit 1.3, hvilket manifesteres i interessentoverblikket. Der er i undersøgelsesdesignet redegjort for specialets afsæt i det teoretiske perspektiv (Bilag [K1]). Dette afsæt har ligeledes betydning for de specifikke undersøgelsesmetoder og deres udformning i henhold til interessentgrupperne. Spørgeskemaer og interviewguides udformning og indhold, tager afsæt i det teoretiske perspektiv, som nævnt i afsnit 1.3 og 2. Indsigt i indholdet af interviewguides og spørgeskemaer kan findes i bilag [D] og bilag [E]. Ligeledes kan specifikke eksempler af det teoretiske perspektivs indblanding i specialets metode findes i afsnit 3.5. Ydermere vil dette afsnit redegøre for antallet af interessenter fra de tre interessentgrupper: cyberværnepligtige, aftagerorganisationer og rammesættende organisationer.

- De rammesættende interviewpersoner er udvalgt specifikt for at opnå forståelse for den nationale cyberindsats, hvilken rolle Forsvaret spiller heri, og et myndighedsperspektiv på Forsvarets Cyberværnepligt. Eftersom disse interview ikke er direkte koblet til evalueringen af de cyberværnepligtiges kompetencer, men til at sætte kompetencerne i perspektiv, er disse interessenter ikke udvalgt i antal for at opnå et mætningspunkt, men derimod for at nuancere cyberværnepligtens formål fra flere hierarkiske niveauer.

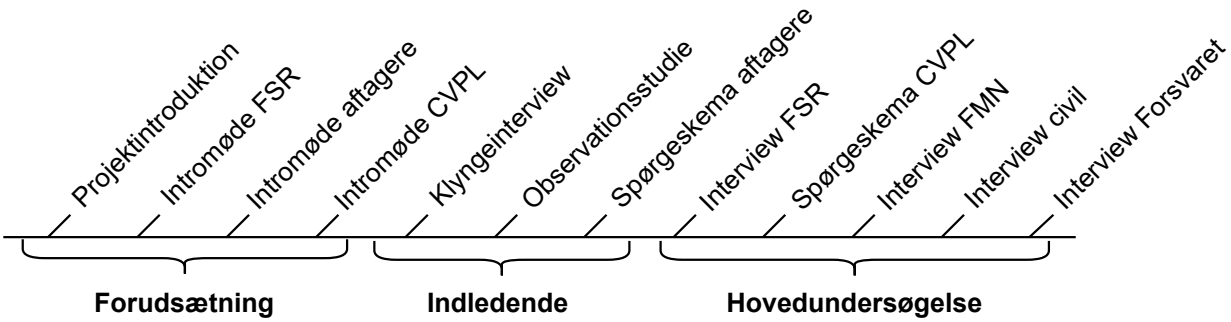
- Vedrørende de cyberværnepligtige som en overordnet interessentgruppe, er disse tilgået ud fra flere metodiske greb. Som samlet interessentgruppe, har de cyberværnepligtige fået tilsendt spørgeskema til besvarelse. Dette er for at indfange så stor en kvantitet af besvarelser som muligt. Derimod bruges de kvalitative metoder primært som en nuancering af den kvantitative data, hvor særligt observationsstudiet nuancerer det resterende datas selvevaluerende grundlag. De kvalitative metoder er kun udført sammen med Hold 7 grundet praktiske omstændigheder.
- Antallet af respondenter tilhørende gruppen af aftagere er todelt: til de kvalitative interviews, er antallet af interviewpersoner fra denne gruppe fastsat ud fra opnåelse af et mætningspunkt i information, hvorefter antallet af interviewede interessenter vurderes fyldestgørende. Til de kvantitative metoder for dataindsamling hos aftagerne, er antallet af respondenter afgrænset af sampling-tilgangen. Dette medfører, at antallet af deltagende respondenter i aftagernes spørgeskema er større end de syv interviewpersoner (IP 4-10).

Det fundamentale grundlag for interessentudvælgelsen og dertil brugte metoder, skyldes den kritiske realismes epistemologiske afsæt i at ville forstå kompleksiteten og fortolkningen af den ellers objektive virkelighed. Metoderne er derfor udvalgt til både at forstå den empiriske virkelighed, og gennem en pluralisme af interessenter med både direkte og indirekte relation til cyberværnepligten, vil dybere lag i den komplekse virkelighed kunne tilgås og erkendes.

Interessentoverblik

I dette afsnit dannes et visuelt overblik over hhv. hvilke interessenter er samplet, hvilket metodisk greb er foretaget for at generere data, og til sidst hvilket formål interessenten har til at besvare underspørgsmål. Det visuelle overblik har til hensigt at opnå transparens, hvilket indgår som kvalitetskriterie jf. afsnit 3.1.1.

Figur 3.3 viser i hvilken del af undersøgelsen den enkelte interessentgruppe indgår. I figuren inddeles undersøgelsen i tre dele, herunder de forudsætningsskabende undersøgelser, indledende- og hovedundersøgelse.



Figur 3.3: Interessenter i undersøgelsesdesign

Tabel 3.1 uddyber for den enkelte interessent forkortelsesnavn, stilling, undersøgelsesmetode, enhed, formål, samt referencer til bilag, hvor dataen for den specifikke interessent forefindes.

Hvem	**Stilling**	**Metode**	**Enhed**	**Formål**	**Bilag**
CVPL	CVPL hold 7	Klyngeinterview, observationsstudie, spørgeskema	Nuværende CV-PL	Underspørgsmål 1-3	C1-3; D6; E1-2; F2;
CVPL	CVPL hold 8	Spørgeskema	Nuværende CV-PL	Underspørgsmål 1-3	E1-2; F2
CVPL	CVPL hold 1-6	Spørgeskema	Tidligere CVPL	Underspørgsmål 1-3	E3-4; F3
IP 4-9 andre	Ledere/rådgivere	Spørgeskema	Civile/militære aftagere	Underspørgsmål 1-3	E5-6; F4
IP 1	Officer	Interview	Føringsstøtte-regimentet	Rammesættende	A1; B1-4; D3
IP 2	Chef CFCS	Interview	CFCS	Rammesættende	A2; B1-4; D4
IP 3	Fuldmægtig	Interview	Forsvars-ministeriet	Rammesættende	A3; B1-4; D5
IP 4-7	Ledere/rådgivere	Interview	Civil aftager	Underspørgsmål 1-3	A4-7; B5-10; D1
IP 8-9	Leder	Interview	Militær aftager	Underspørgsmål 1-3	A8-9; B5-10; D1
IP 10	Underviser	Interview	Civil aftager	Underspørgsmål 1-3	A10; B5-10; D2

Tabel 3.1: Interessentoverblik

3.3 Særlig adgang

Specialet er skrevet i samarbejde med Føringsstøtteregimentet, og undersøger en case i Forsvaret. Den metodiske selvrefleksion hertil, retter sig mod at det vil være yderst svært at replikere undersøgelsen, uden undersøgere med samme adgang. Afsnittet fremhæver metoden, der bidrager med klarhed og transparens over, hvordan undersøgelsen er udført.

Casen kan ifølge Flyvbjerg beskrives som en ekstrem case (Flyvbjerg, 2010), hvor de dybere problemer og konsekvenser undersøges, hvilket kun er muligt gennem den særlige adgang til casens interessenter. Den særlige adgang til casen var mulig, da en af forfatterne bag specialet har haft en længerevarende professionel tilknytning til Forsvaret og dermed indgående kendskab til organisationen, samt et eksisterende netværk heri. Det bygger tildels på, at den omtalte forfatter har en fortid i en højt respekteret og anerkendt afdeling, hvilket formodes at påvirke samarbejdsvilligheden og adgang til de interessenter, der indgår i undersøgelsen. I forlængelse heraf, vurderes det også, at tilslutning og opbakning til deltagelse i specialet er påvirket af denne faktor. Dette kommer f.eks. til udtryk i form af, at flere af dataindsamlingsmetoderne er foregået på steder

eller med personer, der ellers er notorisk lukkede og utilgængelige for offentligheden. Det gør sig gældende for både den rammesættende del, cyberværnepligtige og aftagersiden. Det understreges, at der er i forbindelsen med undersøgelsen ikke indhentet eller anvendt fortrolige oplysninger jf. Forsvarets klassifikationssystem. Hertil giver afsnit 3.2 et overblik over hvilke interviewpersoner, som undersøgelsen har givet adgang til.

Interviewperson	**Stilling**	**Organisation**	**Interessenttype**
IP 1	Officer	Føringsstøtteregimentet	Rammesættende
IP 2	Chef	Center for Cybersikkerhed (CFCS)	Rammesættende
IP 3	Fuldmægtig	Forsvarsministeriet	Rammesættende
IP 4	Leder	Sundhedsdatastyrelsen, offentlig kritisk infrastruktur	Civil Aftager
IP 5	Senior Advisor	Privat kritisk infrastruktur, 23.000 ansatte	Civil Aftager
IP 6	Senior Advisor	Privat kritisk infrastruktur, 4.600 ansatte	Civil Aftager
IP 7	Operational Manager	Leverandør til kritisk infrastruktur	Civil Aftager
IP 8	Ekspert	Cyberdivisionen (FMI)	Militær Aftager
IP 9	Teknisk Officer	Søværnet	Militær Aftager
IP 10	Professor, Underviser	Aalborg Universitet	Civil Aftager

Tabel 3.2: Overblik over interviewpersoner

Med afsæt i Bansal & Sharma (2020), hvor en lignende situation udspilles, vurderes *særlig adgang* ikke at være problematisk, men i stedet forudsætningsskabende. I undersøgelsen skyldes det, at specialets omtalte forfatter ikke er en del af den daglige gang hos interessentgrupperne. Derudover er forfatterskab, interaktioner, spørgeskemaer og interviews udformet og udført i fællesskab i specialegruppen. Den omtalte forfatters unikke adgang har igennem undersøgelsens interne kollaborative elementer ikke skadet integritet og kvalitet, da der har været et miks af insider- og outsider tilgang (Sharma og Bansal, 2020, s. 390). Den har blot fungeret, som en mulighed for netop at opnå unik adgang.

3.4 Bias

Der er i alle typer af studier risiko for bias. Kvalitative studier giver dybde, mens kvantitative studier med store N-værdier giver bredde. Kvalitative undersøgelser og casestudier bliver ofte kritiseret som videnskabelig metode, men denne holdning bygger på en forkert grundforståelse af casestudiets værdi og formål, og er ifølge Flyvbjerg (2010, s. 481-487) ikke mere udsat for verifikationsbias af forudindtagede meninger end kvantitative metoder. For at imødekomme bias-problematikker anvendes et kombineret design jf. 3.5. Det vurderes dog, at der eksisterer bias indenfor især nedenstående områder ved den anvendte metodologi.

Bias i casestudiet

Casestudiet, hvilket også er tilfældet i specialet, bygges ofte på forståelse og læring omkring fænomener. Hertil indgår en naturlig læringsproces, hvor både forsker og fænomen indgår naturligt i denne proces (Flyvbjerg, 2010, s. 481). Derved erkendes en form for subjektivitet fra både os som undersøgere og det undersøgte fænomen. Subjektivisme er uundgåelig og nødvendig for at opnå dybde i casen, hvilket også naturligt reflekterer det videnskabsteoretiske ståsted i afsnit 3.1. Dette gensidige læringsforhold ses som en styrke for at opnå bedre resultater, hvilket uddybes i afsnit 4 om evalueringsteori.

Positiv tilslutning

I forlængelse hertil bemærkes, at der har været gennemgående stor og positiv tilslutning til deltagelse i undersøgelsen fordelt på alle interessentgrupper. Der er ligeledes opnået adgang til interessenter på et højt professionelt niveau, hvilket indikerer en interesse fra respondenters side for at deltage i undersøgelsen. Dette tolkes som en udpræget interesse i at belyse fænomenet cyberværnepligt fra de deltagende interessenter, hvilket kan have ført til, at respondenter i høj grad ønsker deres holdning udtrykt. En overvejelse om den gennemgående positive deltagerinteresse, kan have påvirket os som undersøgere og dermed introducere et bias ift. hvor kritisk respondenterne tilgås.

Bias for særlig adgang

Dertil må den beskrevne adgang i afsnit 3.3 antages at spille en rolle og potentiel bias, der opstår ved en form for autoritet og karisma omkring det forhold der har skabt "særlig adgang". Der er risiko for, at vi som undersøgere bliver mødt anderledes, end hvis denne validering ikke var opnået. Samtidigt bygger adgangen til respondenter netop på dette forhold, og derfor må det samlet set tolkes som en positiv forudsætningsskabende mekanisme. Risikoen for denne bias, opvejes af måden hvorpå forfatterskab, dataindsamling og behandling er blevet udført jf. afsnit 3.3.

Bias ved intern validering ved interessenter

Det vurderes, at der sandsynligvis har foregået en form for intern validering på respondentsiden, af selve undersøgelsen, og dermed også en samlet interesse i at deltage. Det skyldes tildels *snowballsampling* beskrevet i afsnit 3.2.1, men også at casens interessenter kender hinanden og indgår i netværk med hinanden, hvori der kommunikeres internt, og undersøgelsen rygtes. Dette kan potentielt yderligere forbindes til den "særlige adgang"og dermed introducere et bias til respondenters svar.

3.5 Dataindsamling - mixed-method

Dette afsnit har til formål at beskrive, hvordan empiri indsamles kvalificeret til at besvare problemformuleringen fra afsnit 1.1. Med afsæt i undersøgelsens videnskabsteoretiske positionering, *kritisk realisme* fra afsnit 3.1, anvendes i dataindsamlingen en *Mixed-methods* tilgang. Dette er i kraft af, at virkeligheden opfattes som værende kompleks, og forekommende i flere epistemologiske lag. Mixed-methods-tilgangen gør det muligt at evaluere cyberværnepligten gennem kombination af flere forskellige dataindsamlingsmetoder, hvilket bidrager med nuancerede og dybdegående besvarelser af underspørgsmålene. Mixed-methods tilgangen tager udgangspunkt i Venkatesh et. al.s (2023) rammeværk til kombinering af kvalitative og kvantitative empiriindsamlingsmetoder. I dette afsnit beskrives, hvordan metoderne kombineres og segmenteres i indledende- og hovedundersøgelse, som vist i figur 3.3. Der diskuteres yderligere i dette afsnit, hvorfor og hvordan de udvalgte metoder kombineres, dog beskrives den enkelte metode ikke yderligere. En dybere beskrivelse af den enkelte metode med dertilhørende teoretisk grundlag forefindes i bilag [I1].

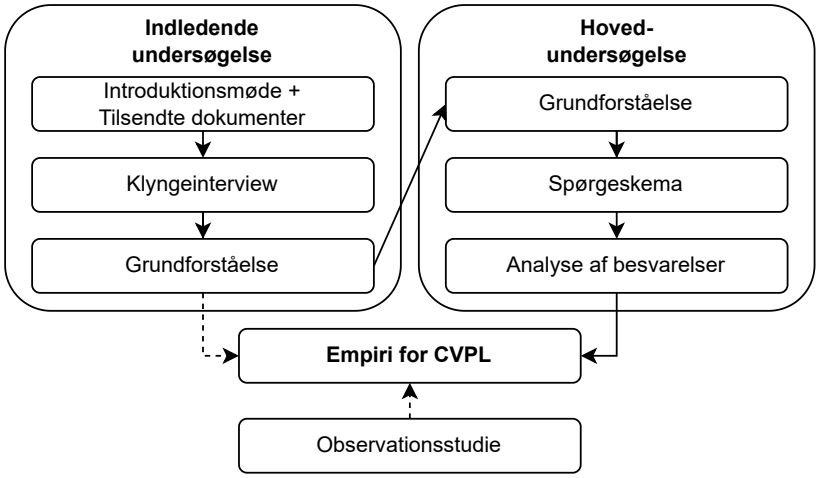
Undersøgelsen søger at besvare underspørgsmålene igennem undersøgelsesdesignet beskrevet i afsnit 1.3, hvor tre primære interessentgrupper forekommer. De tre interessentgrupper tilgås igennem tre separate empiriindsamlingsprocesser, og beskrives derfor ligeledes separat i dette afsnit.

3.5.1 Cyberværnepligtige

Ifølge undersøgelsesdesignet i afsnit 1.3, ønskes det at evaluere de cyberværnepligtige. Ydermere ønskes det, som følge af den abduktive tilgang beskrevet i afsnit 3.1.1, at stille sig åben overfor nye problemstillinger, forbedringsmuligheder eller lignende i mødet med de cyberværnepligtige. Til dette anvendes Venkatesh' et. al. (2023) rammeværk for mixed method design, hvor et *Partially Mixed Sequential Quantitative-dominant status* design udvælges på baggrund af figuren, som findes i bilag [I2] (Venkatesh, Brown, og Sullivan, 2023, s. 93). Designet har *Developmental Purpose* som formål, hvor den kvalitative undersøgelse bruges til at udvikle forståelse for problemstillingen. Denne forståelse anvendes efterfølgende til at udarbejde en kvalificeret kvantitativ undersøgelse, som har hovedvægt i undersøgelsen af de cyberværnepligtige. Designet anvendes derved m.h.p. at øge validiteten i undersøgelsen (Venkatesh et al., 2023, s. 66-67).

Figur 3.4 beskriver, hvordan designet bruges til at undersøge de cyberværnepligtige i praksis. Indledningsvist dannede uddannelsesbeskrivelsen (bilag [G3]), et introduktionsmøde (bilag [G1]), og figur 1.1, grundlag for et indledende klyngeinterview med de cyberværnepligtige.
Klyngeinterviewet blev udvalgt m.h.p. at indsamle en bred vifte af perspektiver på cyberværnepligten på overkommelig vis. Metoden er fordelagtig tidligt i undersøgelsesforløbet, hvor problemfeltet afdækkes. Interviewguide til klyngeinterview findes i bilag [D6]. Disse kvalitative informationskilder danner i kombination grundlaget til den kvantitative undersøgelse, som består af et spørgeskema til de nuværende og tidligere cy-

berværnepligtige. Ydermere opstod også muligheden for at lave observationsstudie på de cyberværnepligtige til deres afsluttende prøve. Observationsstudiet (Se bilag [C2] og [C3]) indgår også til at nuancere besvarelserne fra spørgeskemaet, dog ligger hovedvægten i undersøgelsen stadig i spørgeskemaet, eftersom antallet af respondenter her er markant større, som vist i tabel 3.1.
Samlet set forstås de cyberværnepligtige derfor igennem den indledende kvalitative undersøgelse, den kvantitative hovedundersøgelse og observationsstudiet, hvor hovedundersøgelsen vejer tungest.

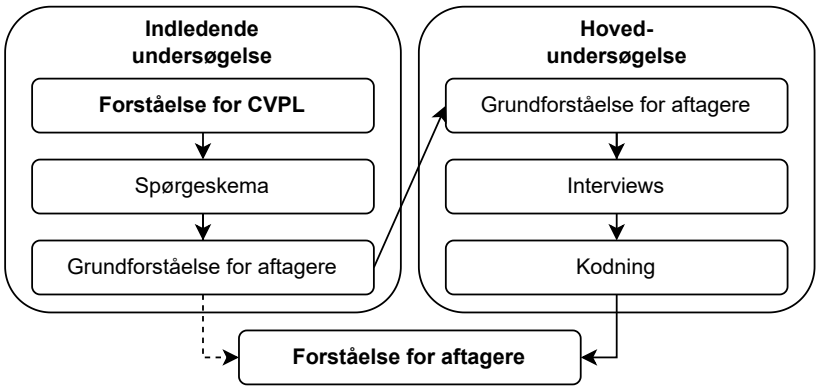


Figur 3.4: Qualitative-quantitative mixed-method design
(Venkatesh et al., 2023, s. 86)

3.5.2 Aftagere

Til at undersøge aftagerne af de cyberværnepligtige, anvendes igen Venkatest et al.s (2023) rammeværk for mixed-method design. Dog anvendes i stedet *Partially Mixed Sequential Qualitative-dominant status* design med *development purpose*. I dette design anvendes en kvantitativ undersøgelse indledningsvist, hvorefter en kvalitativ undersøgelse, som har hovedvægt i undersøgelsen, udarbejdes og kvalificeres på baggrund heraf. Denne tilgang er valgt, eftersom antallet af aftagere var væsentligt mindre end antallat af nuværende eller tidligere cyberværnepligtige jf. tabel 3.1, hvormed det mulige empirigrundlag for en kvantitativ undersøgelse er mindre. Ydermere var aftagernes tilhørsforhold til cyberværnepligten ukendt, hvilket gjorde det muligt at frasortere aftagere, som ikke havde dybere kendskab til cyberværnepligten, igennem spørgeskemaet.

I figur 3.5 ses hvordan mixed-method designet blev udført i praksis. Den indledende kvantitative del bestod af et spørgeskema til aftagerne (bilag [E5]), som baseres cyberværnepligten jf. afsnit 3.5.1. Spørgeskemaet dannede en grundforståelse for aftagerne, hvor de blev udvalgt via *criterion sampling* beskrevet i afsnit 3.2.1. De udvalgte aftagere indgår i hovedundersøgelsen, i form af semistrukturerede interviews (bilag [D1-D2]). Forståelsen for aftagerne dannes derfor ud fra en kombination af det kvantitative spørgeskema, og de kvalitative interview, hvor den kvalitative del er hovedvægtig.



Figur 3.5: Quantitative-qualitative mixed-method
(Venkatesh et al., 2023, s. 85)

3.5.3 Rammesætning

De rammesættende interessenter, i modsætning til aftagerne og de cyberværnepligtige, blev ikke undersøgt igennem et mixed-method undersøgelsesdesign, men i stedet gennem separate semistrukturerede interviews. Et mixed-method undersøgelsesdesign blev fravalgt, eftersom de rammesættende interessenter ikke direkte indgår i forholdet mellem de cyberværnepligtige og aftagerne jf. afsnit 1.3, hvorfor separate semistrukturerede interviews blev vurderet tilstrækkeligt. Interviewguides til de semistrukturerede interviews blev udarbejdet på baggrund af forskellige dokumenter, samt den forforståelse for rammesætningen, som gjorde sig gældende på daværende tidspunkt. De specifikke dokumenter, som det enkelte interview var baseret på, fremgår i de respektive interviewguides (Se bilag [D3-D5]).

3.6 Databehandling

Dette afsnit har til formål at beskrive, hvordan undersøgelsens data fra afsnit 3.5 behandles. Hertil anvendes Gioia, Corley, og Hamilton (2012) rammeværk til behandling af kvalitativ data (Gioia et al., 2012), og Agresti (2018) metode til deskriptiv statistik for behandling af kvantitativ data (Agresti, 2018). Hensigten hermed er at opnå transparens i hvordan undersøgelsens resultater fremkommer, hvilket fremgår som kvalitetskriterie i afsnit 3.1.1. Behanldingen af data er gruppebaseret og kendetegnet ved en vekselvirkning mellem individuel og fælles bearbejdning af data.

3.6.1 Kodning af kvalitativ data

Afsnittet har til formål at klarlægge, hvordan data fra kvalitative interviews er blevet behandlet. Klarhed over fremgangsmåde, metode og slutninger, skal bidrage til at styrke kvaliteten af databehandlingen gennem transparens, der af afsnit 3.1.1 fremgår som kvalitetskriterie. Fremgangsmåde og struktur for databehandling foregår med afsæt og inspiration i Gioia et al. (2012).

Den transparente og strukturerede databehandling fører til øget robusthed og bidrager dermed til kvalitetskriterierne (Gioia et al., 2012, s. 16, 20). For at leve op til kvalitetskriteriet om en gennemsigtig proces, foregår databehandling i nedenstående 5 trin, der samlet set er med til at kondensere indholdet i en struktureret proces fra interviews til aggregerede dimensioner.

1. Transskribering: De 10 kvalitative interviews (3 rammesættende & 7 aftagere) transskriberes alle i fuld længde, hvilket skaber forudsætningen for efterfølgende behandling af empiri (bilag [A1-A10]). Metoden skaber desuden et samlet overblik over det empiriske materiale for både læsere og undersøgere.

2. Åben kodning af første orden koncepter: Denne fase er baseret på en induktiv tilgang. Der ledes ikke efter teoretiske begreber og koncepter (Gioia et al., 2012, s. 20). Dog anderkendes det, at der med afsæt i de semistrukturerede interviews er prædefinerede koncepter, der med sikkerhed vil opstå. Dog er selve indholdet af dem ukendt, og derfor argumenteres for at metoden fastholdes i en induktiv tilgang. Se bilag [B1-B10].

3. Sammenfatning af første ordens koncepter på tværs af interviewpersoner i temaer (anden ordens kodning):
Koncepter samles på tværs af alle interviewpersoner, hvor der målrettet ledes efter ligheder og forskelligeheder heri. Metoden reducerer datamængden til en mere overkommelig størrelse med generel karakteristika (Gioia et al., 2012, s. 20). Det betyder desuden, at der på en simpel måde opnås mulighed for at manøvrere i meget store datamængder (Brinkmann, 2020, s. 319). I praksis udføres denne fase for hhv. militære og civile aftagere af cyberværnepligtige (Se bilag [L1-L2]).

4. Lukket kodning i anden orden udført som selektiv kodning: Fasen udføres med afsæt i en mere deduktiv tilgang, hvori de mest fremtrædende koncepter hjælper til at forstå og forklare undersøgelsesfænomenet (Brinkmann, 2020, s. 56, 315-316). Fasen burde være forankret i et teoretisk domæne jf. (Gioia et al., 2012, s. 20), men her afviges fra Gioia et al. (2012), eftersom der ikke findes en enkeltstående teori for undersøgelsesfænomenet. I stedet arbejdes der i en deduktiv retning med afsæt i formål med cyberværnepligten gennem officielle dokumenter samt det teoretiske perspektiv. Resultatet af processen er tværgående temaer. Se bilag [L1-L2].

5. Kondensering af temaer i aggregerede dimensioner Slutteligt destilleres de tværgående temaer til aggregerede dimensioner, der er en fællesbetegnelse for temaer der naturligt hører under samme område. Disse vil naturligt være af mere deduktiv karakter, eftersom der målrettet ledes efter ligheder og teoretisk forankring jf. (Gioia et al., 2012, s. 20), men her afviges der igen metodisk mod en empirisk forankring i de officielle dokumenter som f.eks. (Forsvaret, 2023a).

Det anerkendes, at processen på trods af dens rigide struktur med afsæt i Gioia et al. (2012) vil medføre, at data konstrueres gennem den beskrevne kodeproces (Brinkmann, 2020, s. 315), og indeholder en grad af subjektivitet, der påvirker objektiviteten og reliabiliteten ved fremgangsmåden. Det kan dog forsvares i, at metoden ikke har til hensigt at klarlægge entydige årsager og sammenhæng (Brinkmann, 2020, s. 315).

3.6.2 Behandling af kvantitativ data

Undersøgelsens formål er at forstå en kompleks problemstilling, der har afsæt i en række aftagere. Formålet er grundigt at forstå fænomenet cyberværnepligt fremfor at lave forudsigelser om fremtiden og kunne generalisere på tværs af populationen. Til en kompleks problemstilling som denne, findes en deskriptiv tilgang relevant. Desuden er det med undersøgelsens sample, beskrevet i afsnit 3.2.1, naturligt at anvende kvantitativ data med deskriptivt formål, da samplet ikke tillader generaliserbarhed ud over den undersøgte polulation.
Den deskriptive statistik fokuserer på at opsummere data og gøre det letforståeligt gennem mere simple statistiske metoder (Agresti, 2018, s. 17), hvilket vil være den gennemgående fremgangsmåde under behandling af dette for at frembringe generelle tendenser i det undersøgte sample. Der fokuseres derfor på frekvens, forekomst, gennemsnit, fordelinger mv. Den deskriptive statistik er desuden velegnet, når hele populationen er tilgængelig, og det rent faktisk er muligt at foretage generalisering på tværs af denne (Agresti, 2018, s.17), hvilket den er i kategorien *nuværende cyberværnepligtige*. Valget af fremgangsmåde med deskriptiv statistik findes derfor anvendelig og velegnet i relation til både formål med undersøgelsen og i forhold til de respondenter, der har været tilgængelige for casen.

Likert skala

I dele af spørgeskemaet bedes informanterne vurdere enigheden i en række udsagn. Graden hvormed informanten er enig, kvantificeres herefter gennem brug af likert-skalaen (Benyon, 2019, s.113-117), som illustreret i tabel 3.3 . Likert-skalaen bruges til at beregne gennemsnit. En gennemsnitsbesvarelse på 4 betyder derved, at informanterne i gennemsnit er enige i udsagnet. Den fulde behandling af den kvantitative data findes i bilag [F1].

Meget uenig	Uenig	Hverken/eller	Enig	Meget enig	Ikke relevant
1	2	3	4	5	Ikke gyldig

Tabel 3.3: Likert-skala

3.6.3 Behandling af observationsdata

Behandlingen af observationsdata er foregået i to etaper: Første behandling af observationsdataen er foregået *in situ* under selve observationen. Dette manifesteres ved, at feltnoterne har tre datakolonner: Ét hvor den umiddelbare observation beskrives, sådan som den er sanset; efterfulgt af en kolonne med en antagelse om, hvad observationen er udtryk for; og til sidst en fortolkning af denne antagelse, hvor observatør tillægger egen fortolkning af, hvad observationen kan antages at betyde (Se bilag [C3]).
Anden etape i behandling af observationsdataen er foregået efter observationen. Den indsamlede data kategoriseres på tværs af sites i 4 kategorier: organisatorisk, ledelsesmæssig og tekniske kompetencer, samt profil. De samlede kategorier farvekodes efterfølgende, for at finde gennemgående tematikker i hver af de 4 kategorier (Se bilag [C2]).

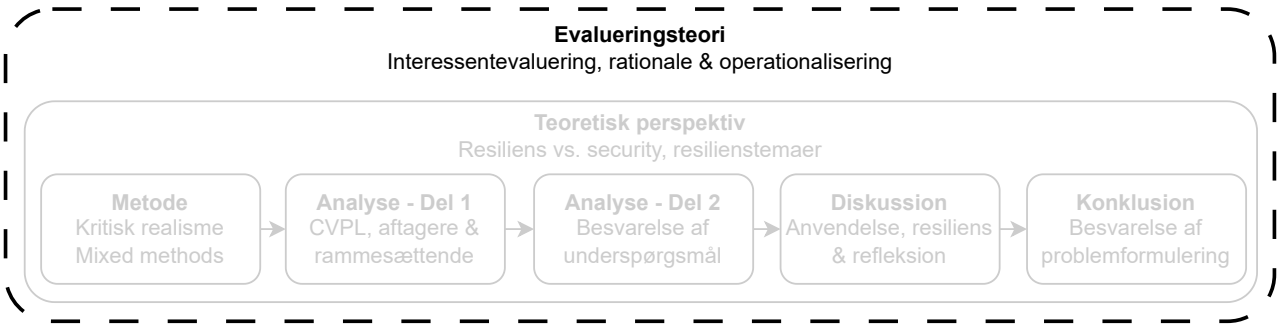
3.6.4 Behandling af klyngeinterviews

Dette afsnit har til formål at beskrive, hvordan klyngeinterviewdataen fra hold 7 behandles. Dataen fra klyngeinterviewet består af noter, som blev taget imens mødet blev afholdt, samt supplerende pointer, som blev opfanget ved at genhøre de to klyngeinterviews. Dataen kodes ved brug af samme metodik som de øvrige interviews, hvilket står beskrevet i afsnit 3.6.1. Dog transkriberes klyngeinterviewet ikke, eftersom det ønskes at danne et helhedsbillede af cyberværnepligten, og det derved ikke er relevant at bestemme hvilke(n) cyberværnepligtig, som kommer med en bestemt udtalelse. Herefter foretages ligeledes en åben kodning, sammenfatning af koncepter, lukket kodning, samt en kondensering af teamer. Kodningen af noterne fra klyngeinterviewet findes i bilag [C1].

Kapitel 4

Evalueringsteori

Dette kapitel har til formål at udfolde det teoretiske grundlag for en systematisk evaluering af cybervær-nepligtens relevans, som tager udgangspunkt i undersøgelsesdesignet fra afsnit 1.3. Som beskrevet i afsnit 1.3 og vist i figur 4.1, indgår evalueringsteorien ikke sekventielt som de øvrige afsnit, men er i stedet omkringliggende og rammesættende for undersøgelsen. Indledningsvist udfoldes det teoretiske grundlag for evaluering indenfor casens ramme, hvorefter evalueringstilgangen operationaliseres i praksis. Evalueringsteorien fremgår derfor som et separat kapitel, som er influeret af de metodiske valg, og som har haft betydning for analysens struktur. Alt dette m.h.p. at besvare undersøgelsesdesignets spørgsmål.



Figur 4.1: Evalueringsteoriens placering i undersøgelsen

4.1 Evalueringsrationale

I udformningen af en praktisk evalueringsstrategi, har både undersøgelsesdesignet og de metodologiske grundrammer været dikterende for hvilken type evalueringstilgang, som udvælges til at forstå cyberværnepligtens relevans.
Jf. Krogstrups (2016) rammeværk for evaluering, må casen erkendes som værende kompleks, eftersom der ikke forekommer klare regler eller opskrifter for, hvornår cyberværnepligten kan opfattes som værende succesfuld/relevant (Krogstrup, 2016, s. 25-27). Grundet dette, er evalueringstilgangen udformet med henblik på at indfange et undersøgelsesområde, hvor en divers samling af interessenter, hver især tillægger cyberværnepligten værdi afhængig af deres egen individuelle kontekst. Særligt fokuseres på aftagerorganisationer, de cyberværnepligtige og de rammesættende interessenter, som direkte eller indirekte påvirker cyberværnepligten. Som følge heraf, baseres evalueringen på det typiske interaktive evalueringsparadigme, hvor evaluator og relevante interessenter interaktivt evaluerer cyberværnepligtens relevans med udgangspunkt i interessenternes egen kontekst (Bredgaard, 2016; Krogstrup, 2016, s. 217-218, s. 155-156).

I handling sker evalueringen med afsæt i den kritisk realistiske videnskabsfilosofi, hvor den objektive virkelighed samtidig opfattes som kompleks og kontekstuel, som beskrevet i afsnit 3.1. Dette medfører en operationalisering af evalueringen som teoretisk paradigme og model, der er formet m.h.p. at være brugbar i kontekst af undersøgelsesdesignet. Dette betyder, at evalueringen er modificeret, tilpasset og abstraheret i det omfang, der har været relevant for at besvare underspørgsmålene. Hvorfor, hvornår og hvordan evalueringstilgangen er modificeret og tilpasset, vil blive udfoldet i afsnit 4.2.

4.1.1 Det interaktive evalueringsparadigme

Den primære evalueringslogik i undersøgelsen er baseret på en tilpasset udgave af den interaktive evalueringspraksis, som er en samlebetegnelse for de dialogbaserede evalueringsperspektiver (Bredgaard, 2016, s. 217). Som navnet antyder, defineres den interaktive evalueringstilgang ud fra en omfattende interaktion imellem os som evaluator og cyberværnepligtens interessenter (Krogstrup, 2016, s. 155-156). Formålet med at bruge interaktiv evaluering er, at aktivt samarbejde med interessenter i at engagere dem i cyberværnepligtens aspekter. Hver interessent har deres egne subjektive forståelser, fortolkninger og værdier bundet op på de cyberværnepligtige (Krogstrup, 2016, s. 155-156). Denne subjektivitet er unik, ikke bare for cyberværnepligten som case, men for hver interessent og deres egne unikke miljøer. Det er gennem dette, at en dybdegående forståelse for de cyberværnepligtiges kompetencer kan kortlægges og vurderes. Ligeledes er det også disse perspektiver, som giver dybdegående viden for *substansen* af de kompetence- og profilbehov, som de cyberværnepligtige ønskes at kunne indfri (Krogstrup, 2016, s. 166-167). I praksis manifesteres interaktionen særligt gennem interview, hvilket beskrives mere dybdegående i afsnit 4.2.
Ved spørgsmålet om hvordan vi tilgår opnåelse af denne dybdegående viden, drages elementer af den *Responsi-*

ve Evaluering (Bredgaard, 2016, s. 217-224); (Krogstrup, 2016, s. 160-164). Selvom dette er et epistemologisk spørgsmål, er det stadigvæk essentielt for at forstå evalueringens rationale og tankegods. Modeller tilhørende den responsive evaluering, hvordan de bliver operationaliseret og brugt i praksis, fremgår i afsnit 4.2.
Den responsive evalueringslogik er, i sin rendyrkede form, typisk formativt fokuseret, og formet kontinuerligt gennem interaktion med interessenterne i deres respektive kontekster (Bredgaard, 2016, s. 221-224). Opfattelsen er, at perspektiver på sandhed varierer i den kontekst som forskellige interessenter indtager og positionerer sig som (Krogstrup, 2016, s. 161-164). Dette manifesterer sig også i undersøgelsesdesignet, hvor de primære interessentgrupper: de værnepligtige selv og aftagerorganisationerne, fastsættes som de primære perspektiver til at kunne forstå om cyberværnepligten er relevant i forhold til hvad de kan, kontra det behov de skal udfylde.
Denne undersøgelse vil ikke have til intention at skabe en læringsproces gennem evalueringsforløbet, og differentierer sig derfor fra den typiske responsive evaluering. Derimod er intentionen, at evalueringen skal kunne agere værktøj for at vurdere cyberværnepligtens relevans. Derfor påtages en summativ tilgang til evalueringen, hvor de cyberværnepligtiges kompetencer og profil evalueres som resultatet af en færdiggjort uddannelse, og ikke som en løbende læringsproces i sig selv, som kendetegner en formativ evaluering.

4.1.2 Evalueringsmodeller

Med afsæt i det forhenværende teoriafsnit om evalueringsteoriens rationale, vil det efterfølgende afsnit søge at operationalisere evalueringen i praksis. Dette indebærer en beskrivelse af brugte evalueringsmodeller, hvordan disse er tilpasset vores behov, samt en beskrivelse af evalueringens brug i praksis. Med dette formål, er to modeller med fordel udvalgt fra den responsive evalueringslogik: Interessentmodellen og BIKVA-modellen.

4.2 Operationalisering af evalueringsmodeller

Formelt vil modellerne abstraheres i konteksten af evalueringsformålet, hvorefter modellernes abstraktioner vil sammenflettes i en syntese for at opnå en integreret model. Modellen indeholder kombinerede elementer fra de originale modellers ræsonnement, men som opfylder de behov for udførelse som gør sig gældende for den summative anvendelse. I praksis skal den integrerede model anses mere som et samlet perspektiv for en tilpasset evalueringstilgang, end en reel repræsentation for klare metodiske trin eller faser.

Interessentmodellen

Interessentmodellen inddrager elementer, som med fordel vil inddrages i evalueringsperspektivet. Først og fremmest anses evalueringsområdets situation som komplekst, hvor evaluandens interessenter varetager værdifulde indsigter om områdets kompleksitet, som er unik til den specifikke interessent. Hertil opfattes interessenterne som værdifulde fokalpunkter for viden om de cyberværnepligtiges kompetencer og profil. En viden, som bedst tilgås ved at interagere og indgå i samarbejde. Modellens markante fokus på interessenterne som

primus motor for forståelse, er fundamentet for den integrerede models logik (Krogstrup, 2016, s. 172). Ved specifikt at inddrage cyberværnepligtens interessenter, belyses cyberværnepligten og dens tilsigtede effekter fra så mange vinkler som muligt. Ved hele tiden at evaluere med afsæt i cyberværnepligtens kontekst, samt den kontekst interessenterne befinder sig i, skabes synergering imellem os som evaluatorer og interessenterne. Vi danner vores egne forståelser og fortolkninger baseret på interessenternes perspektiver, hvorfra vores forståelser og fortolkninger forbedres og kvalificerer fremtidig interaktion med interessenterne i empiriindsamlingen. F.eks. er interviewguides løbende udformet på baggrund af tidligere empiriindsamling, eller ud fra besvarelserne i spørgeskema, qua undersøgelsens metodedesign.

Centralt for interessentmodellen er dens omfattende præevaluering, hvor interessenter og deres respektive miljøer kortlægges, og hvor perspektiver udfoldes og sammenfattes (Krogstrup, 2016, s. 172). Særligt præevalueringen er taget centralt ind i evalueringens integrerede model, eftersom alle tænkelige direkte interessenter er blevet både kortlagt og kontaktet m.h.p. empiriindsamling af deres perspektiver. Hvor den integrerede model differentierer sig fra interessentmodellen, er interessentmodellens prioritering af dialogorienterede møder på tværs af interessentgrupper, hvor meninger og perspektiver afstemmes i fællesskab for at opnå en formativ evalueringseffekt (Krogstrup, 2016, s. 171-172). Her afviger den integrerede model fra interessentmodellen delvist. Som tidligere fastslået, er den formative evaluering ikke intentionen med evalueringen. Derfor vil interessentgrupperne ikke indgå i en fælles dialog, bl.a. fordi det er tilnærmelsesvist umuligt at koordinere på tværs af interessentgrupperne. Derimod abstraheres denne fase til vores fordel; styrken ved denne fase er, at introduktionen af andre perspektiver igangsætter refleksion hos interessenterne, som udmunder sig i en mere reflekteret respons, samtidig med at de andre perspektiver er medvirkende til at kvalificere vores, evaluators, interaktion med andre interessenter. Derfor vil interessenterne ikke indgå i fællesdiskussion med deres respektive perspektiver, men i stedet vil perspektiverne blive inddraget af os som evaluator i vores interaktion med andre interessenter. De resterende faser i interessentmodellen vurderes til at være irrelevante for vores evalueringstilgang, og vil derfor ikke benyttes, da de udelukkende fokuserer på formative og dialogbaserede resultater (Krogstrup, 2016, s. 171-173).

BIKVA-modellen

BIKVA-modellen, hvis akronym er '**B**ruger**i**nddragelse i **Kva**litetsvurdering', indeholder ligeledes elementer, som vil give evalueringstilgangen en større dybde (Krogstrup, 2016, s. 176-178). Selvom fokus ikke er specifikt på de cyberværnepligtige som brugergruppen, så fokuseres derimod på *aftagerne* som brugere af de cyberværnepligtige. Dette skyldes, at vi ikke undersøger uddannelsens didaktiske forhold. Med dette in mente, så vil aftagerne opfattes og tilgås som den brugergruppe, hvis indsigter er kvalificerende for at vurdere de cyberværnepligtiges kvalitet. Dette underbygges af, at det er aftagerne som ansætter de cyberværnepligtige m.h.p. at gøre brug af deres kompetencer og profil. Denne ibrugtagen må, alt andet lige, give et kvalificeret perspektiv på cyberværnepligtens kompetencer og profil, og deraf relevans. Først og fremmest drager vi samme erkendelsesmæssige konklusion som BIKVA; det er brugerne af en indsats, som bedst er i stand

til at vurdere, og dermed også udfordre, både indsatsens indhold, dens implementering, samt den nuværende praksis (Krogstrup, 2016, 176-177). BIKVA-modellen tilskriver, at brugernes perspektiver tematiseres og fremlægges for andre interessenter, der har betydning for indsatsens kvalitet (Krogstrup, 2016, s. 177). Dette er også et element fra BIKVA-modellen som benyttes i den integrerede model, da den kvalitative kodning af interviews, med inspiration fra Gioia (2012), skaber en tematisering af brugernes perspektiver.
Ligesom med interessentmodellen, så fraskrives de komponenter, som indeholder et formativt formål eller praktiske begrænsninger.
Metodisk indeholder BIKVA-modellen flere elementer, hvis ræsonnement flugter med de inddragede komponenter i Interessentmodellen. De inddragede komponenter fra BIKVA udgør den logik, som retfærdiggør fravalget af visse dele af interessentmodellen, ligesåvel som interessentmodellen giver grundlag for, at BIKVA-modellen kan bruges mere fleksibelt i praksis. F.eks. fravælges de faser i interessentmodellen, hvor interessenterne skal indgå i fælles dialog. Her suppleres i stedet med BIKVA-modellen, hvor interessenters perspektiver inddrages i interaktionen med andre interessenter, for løbende at kvalificere undersøgelsen. Omvendt giver en omfattende præevaluering, som er taget fra interessentmodellen, mulighed for at drage fra et større interessentkartotek, så større perspektivgrundlag kan indgå i interaktionsudveksling mellem os som evaluator og perspektiverne fra aftagerne. I praksis har interessentmodellen skabt grundlaget for legitimiteten ved at bruge interessenternes unikke perspektiver for at kunne forklare og afbilde cyberværnepligtens kompleksitet. BIKVA-modellen har i praksis suppleret denne legitimitet ved at retfærdiggøre, at ud af en pluralisme af interessenter, så er aftagerorganisationernes perspektiver unikke i at vurdere kvaliteten i cyberværnepligten. Dette manifesteres både i metoden, men også i opsætning af analysen, hvor indsigter fra hver primær interessentgruppe analyseres adskilt og i separate kontekstuelle perspektiver.

Opsummerende er det metodiske afsæt for evalueringen defineret af en interaktionspræget tilgang til evaluering af cyberværnepligtens relevans. Selvom både interessentmodellen og BIKVA-modellen iscenesætter evaluator som facilitator for dialog (Krogstrup, 2016, s. 171-172, 176-177), er det vores intention i stedet at agere dirigent for orkestreringen af mangfoldige perspektiver. Det er gennem dette rationale, at vi retfærdiggør operationaliseringen af allerede eksisterende og velkendte responsive evalueringsmodeller. Endegyldigt er formålet med evalueringen, at dens resultater kan anvendes til at forstå en kompleks kontekst, hvor varierende opfattelser og perspektiver tegner et dybdegående billede af de cyberværnepligtiges kompetencer og profil, samt de behov som skal udfyldes.

Kapitel 5

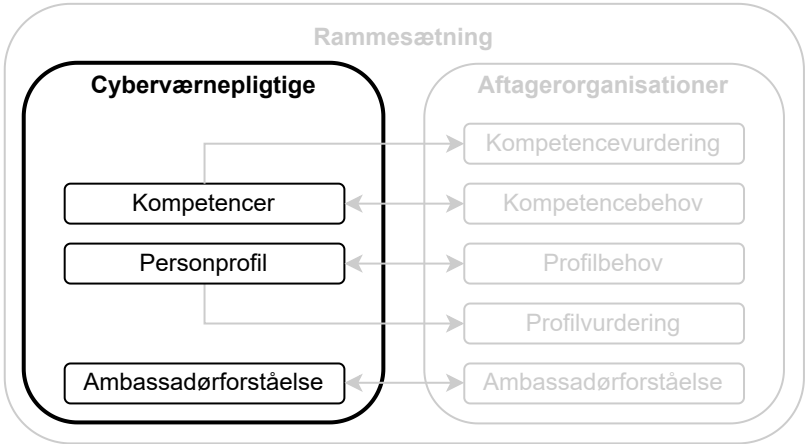
Analyse - Del 1

Analysens struktur tager udgangspunkt i undersøgelsesdesignet fra afsnit 1.3 *(Undersøgelsesdesign)*, hvor de cyberværnepligtige, aftagerorganisationer, samt rammesættende enheder analyseres individuelt, som vist i figur 5.1. Indholdet i analysen af den individuelle interessentgruppe bestemmes ud fra underspørgsmålene, og fremgår af figur 1.3 i undersøgelsesdesignet. Den metodiske tilgang til besvarelse af de tre underspørgsmål, fremgår i afsnit 3.5 *(Dataindsamling - mixed-methods)*, og uddybes løbende gennem metatekster tilhørende den enkelte interessentgruppe. Hensigten hermed er at opnå en dybdegående, transparent analyse.

Figur 5.1: Analyse del 1 i undersøgelsesstrukturen

5.1 Cyberværnepligtige

Dette afsnit har til formål at kortlægge de cyberværnepligtiges kompetencer, personprofil og ambassadørforståelse fra de cyberværnepligtiges eget perspektiv, som vist i figur 5.2.

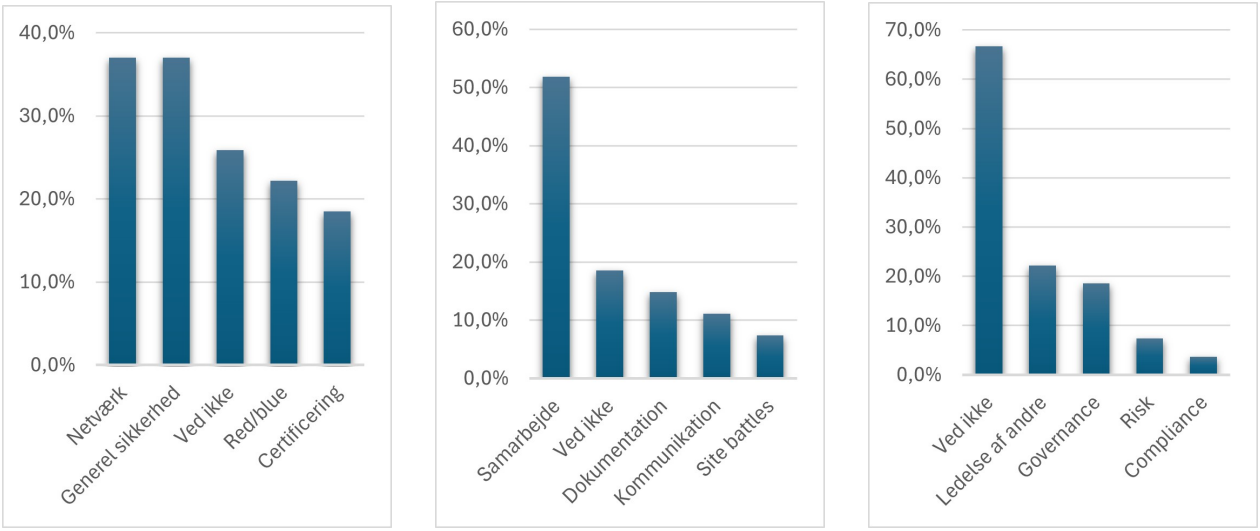


Figur 5.2: Undersøgelsesdesign - Cyberværnepligtige

Hertil anvendes den kvantitative data fra de nuværende og tidligere cyberværnepligtige, samt klyngeinterview og observationsstudie foretaget med cyberværnepligtens hold 7 (bilag [I1]). Den kvantitative data for de nuværende cyberværnepligtige består af spørgeskemabesvarelser fra hold 7 og 8 (bilag E2), mens dataen for tidligere cyberværnepligtige består af spørgeskemabesvarelser fra FDCA-medlemmer (bilag [E4]). Som beskrevet i afsnit 3.5 *(Dataindsamling - Mixed-methods)*, har den kvantitative data hovedvægt i analysen, hvortil klyngeinterviewet (bilag [C1]) og observationsstudiet (bilag [C2-C3]) nuancerer og supplerer fundene.

5.1.1 Kompetencer

De kompetencer, som de cyberværnepligtige selv vurderer uddannelsen bidrager med, undersøges gennem spørgeskemaer, hvor de cyberværnepligtige udfylder de mest fremtrædende tekniske, organisatoriske og ledelsesmæssige kompetencer fra uddannelsen. De hyppigst nævnte kompetencer for de nuværende cyberværnepligtige indenfor det tekniske, organisatoriske og ledelsesmæssige domæne fremgår af figur 5.3a, 5.3b og 5.3c.

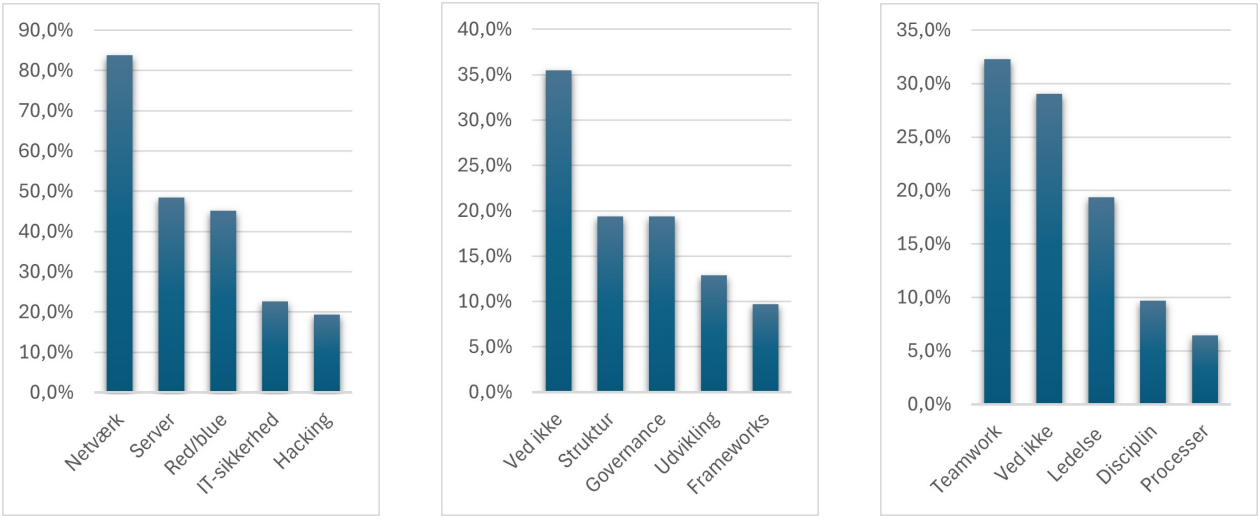


(a) Tekniske (b) Organisatoriske (c) Ledelsesmæssige

Figur 5.3: Nuværende cyberværnepligtiges egen kompetencevurdering

Kompetencerne, som hyppigst nævnes i spørgeskemaet, går igen i klyngeinterviewet, hvor netværksteori ligeledes fremhæves som den væsentligste tekniske kompetence, og governance, risikostyring og red/blue teaming som de væsentligste organisatoriske og ledelsesmæssige kompetencer. I spørgeskemabesvarelserne fremgår det også, at en betydelig del af de nuværende cyberværnepligtige ikke er i stand til at nævne specifikke kompetencer, særligt indenfor det ledelsesmæssige område, hvor 66,7% af de cyberværnepligtige svarer *"ved ikke"*. Spørgeskemabesvarelserne overlapper med observationsdataen, hvor de observerede ledelsesmæssige og organisatoriske kompetencer manifesteret i Hold 7's afsluttende øvelse, der opleves med varierende succes af observanterne. F.eks. udviser størstedelen (3 ud af 4 sites) gode organisatoriske evner til selvstændigt at fordele roller og kommunikere opgaver internt i teamet, men udviser dårlige kompetencer til effektivt at styre en fælles indsats og tage hurtige beslutninger (2 ud af 4 sites). Ligeledes observeres koordinering og planlægning af en fælles strategi med lav intern konsistens, da alle sites observeres med varierende succes i at udforme en strategi og koordinering af et overblik. Vedrørende de tekniske kompetencer, så observeres netværksadministration som en overordnet kompetence, hvor kompetencer som sikkerhedsanalyse og malwareanalyse observeres særligt som fremtrædende tekniske kompetencer, der manifesteres i alle observerede sites. Ligeledes fremstår de cyberværnepligtige som teknisk velovervejet og reflekterende på alle observerede sites.

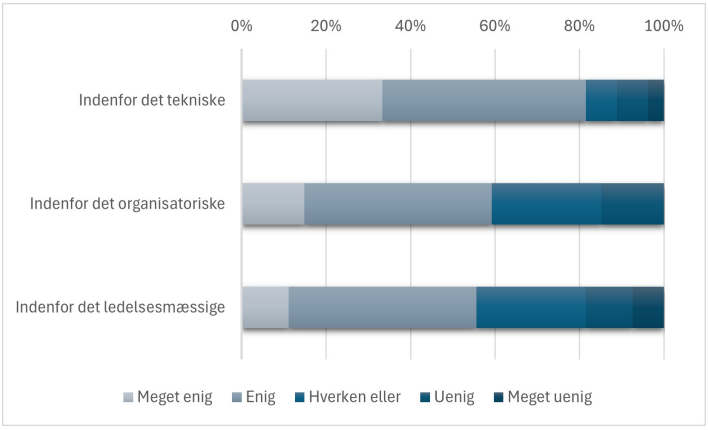
Selv indenfor det tekniske domæne, som cyberværnepligten retter fokus mod jf. afsnit 1.2.1 *(Bag om cyberværnepligten)*, bemærkes det, at 25,9% af de nuværende cyberværnepligtige ikke kan nævne specifikke tekniske kompetencer, som uddannelsen har bidraget med. Dette fortolkes som et udtryk for, at de cyberværnepligtige ikke er bevidste om, hvilke tekniske kompetencer uddannelsen bidrager med. Fortolkningen beror sig på klyngeinterviewet, hvor flere af deltagerne efterspørger i højere grad at være informeret om, hvilke kompetencer der efterspørges i Forsvaret og på det civile arbejdsmarked.
I figur 5.4a, 5.4b og 5.4c fremgår de hyppigst nævnte tekniske, organisatoriske og ledelsesmæssige kompetencer for de tidligere cyberværnepligtige.



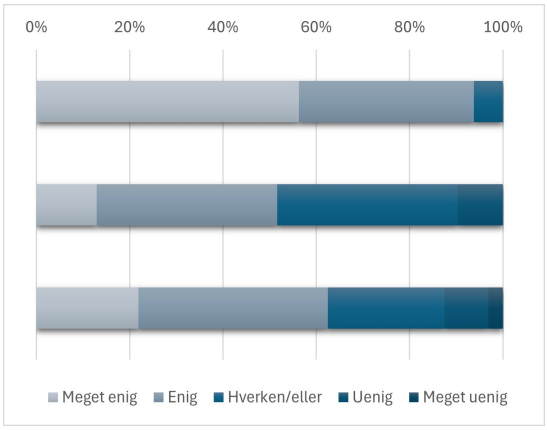
(a) Tekniske (b) Organisatoriske (c) Ledelsesmæssige

Figur 5.4: Tidligere cyberværnepligtiges egen kompetencevurdering

For de tidligere cyberværnepligtige, gør det sig ligeledes gældende, at de hyppigst nævnte kompetencer indenfor de tre domæner er netværk, governance, red/blue teaming, teamwork mv. Dog forekommer en højere detaljegrad i besvarelserne, hvor konkrete værktøjer som SIEM, powershell mv. nævnes, hvorimod de nuværende cyberværnepligtiges besvarelser primært består af mere generelle kompetencer som IT-sikkerhed og netværk. Ydermere er besvarelsesformen *"ved ikke"* ikke anvendt ved de tidligere cyberværnepligtige indenfor det tekniske domæne. Dette indikerer, at der hos de tidligere cyberværnepligtige er sket en udvikling i opfattelsen af egne kompetencer, som har medført, at de i højere grad kan udpege egen kompetenceprofil gennem konkrete eksempler. Denne udvikling understreges i figur 5.5a og 5.5b, hvor det fremgår, hvordan hhv. nuværende og tidligere cyberværnepligtige vægter forholdet mellem egne kompetencer indenfor det tekniske, organisatoriske og ledelsesmæssige domæne.



(a) Nuværende



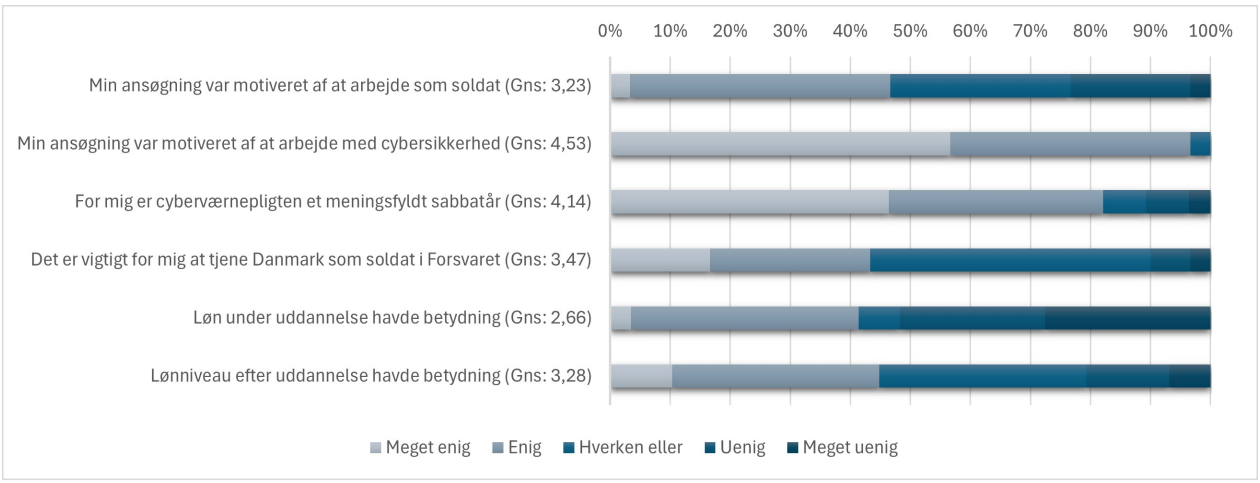
(b) Tidligere

Figur 5.5: Vægtning af kompetencer

I figur 5.5 ses særligt en udvikling i, hvordan de cyberværnepligtige opfatter egne tekniske kompetencer. Her svarer ca. 55% af de tidligere cyberværnepligtige "meget enig"til, at deres kompetencer primært ligger indenfor det tekniske domæne, hvor ca. 30% af de nuværende cyberværnepligtige svarer "meget enig"til samme spørgsmål.

5.1.2 Profil

Til at undersøge de cyberværnepligtiges personprofil, blev det bl.a.undersøgt hvad ansøgningen til cyberværnepligten var motiveret af. Motivationspørgsmålet er kun foretaget på nuværende cyberværnepligtige, hvor ansøgningsprocessen er i frisk erindring sammenlignet med tidligere cyberværnepligtige. Undersøgelsens resultater ses i figur 5.6.

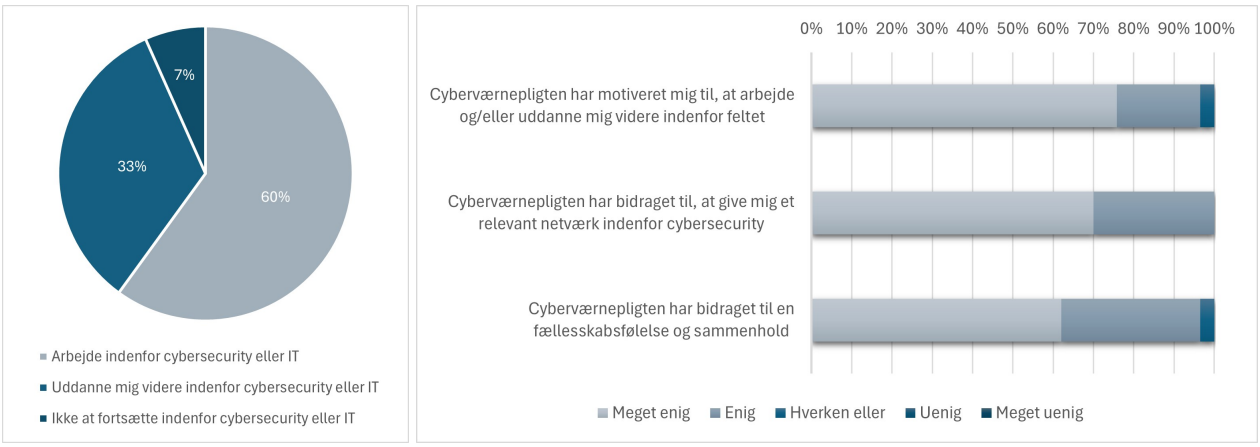


Figur 5.6: Motivation for at søge cyberværnepligten

I figuren fremgår det, at de cyberværnepligtige er særligt motiveret af at arbejdet med cybersikkerhed, hvor gennemsnitsbesvarelsen er 4,5 (enig - meget enig), samt at cyberværnepligten ses som et meningsfyldt sab-

batår med en gennemsnitsbesvarelse på 4,1 (enig). Det fremgår også, at de cyberværnepligtige i mindre grad motiveres af at arbejde som soldat, og at tjene Danmark som soldat, med gennemsnitsbesvarelser på hhv. 3,2 (hverken eller) og 3,5 (hverken eller - enig). Den tekniske interesse understreges ligeledes i klyngeinterviewet, hvor hold 7 udtrykker en fælles grundlæggende interesse for IT, computerspil og programmering. HBU'en anses som værende lærerig og udfordrende, men samtidigt også en engangsoplevelse for de fleste. Det tilføjes hertil, at krav om gennemførsel af Hærens Reaktionsstyrke Uddannelsen (HRU) afholder de cyberværnepligtige fra at fortsætte i Hæren, eftersom de hovedsageligt ønsker at fortsætte indenfor IT og cybersikkerhed. Motivation, som en del af de cyberværnepligtiges personprofil, genkendes også i observationsdataen, hvor de cyberværnepligtige udviser motivation og drive, og går dedikeret til øvelsesopgaven (3 ud af 4 sites). Ydermere udviser de cyberværnepligtige også holdånd, og samarbejder aktivt i deres respektive teams (3 ud af 4 sites), samt udviser beslutsomhed (3 ud af 4 sites), selvom de kan have behov for en guidende hånd for at undgå usikkerhed og forvirring (2 ud af 4 sites).

Interessen for cyberdomænet går ligeledes igen hos de tidligere værnepligtige, hvilket tydeligt afspejles i hvor de cyberværnepligtige fortsætter karrieremæssigt efter endt uddannelse, som vist i figur 5.7a. Ydermere fremgår det af dataen, at cyberværnepligten ses som motivationsgivende for at fortsætte indenfor cybersikkerhed efterfølgende, samt at bidrage med relevant netværk og sammenhold, hvilket fremgår af figur 5.7b.



(a) Fremtidsmuligheder

(b) Cyberværnepligten som motivationsfaktor

Figur 5.7: Betydning af cyberværnepligten

Det fremgår af dataen at 93% af de tidligere cyberværnepligtige er fortsat indenfor cyberdomænet, og at mere end 95% svarer enten meget enig eller enig til, at cyberværnepligten har motiveret til at fortsætte indenfor feltet. Hvor stor en betydning cyberværnepligten har haft, kommer særligt til udtryk igennem tekstfelterne, hvor betydning af uddannelsen udtrykkes:

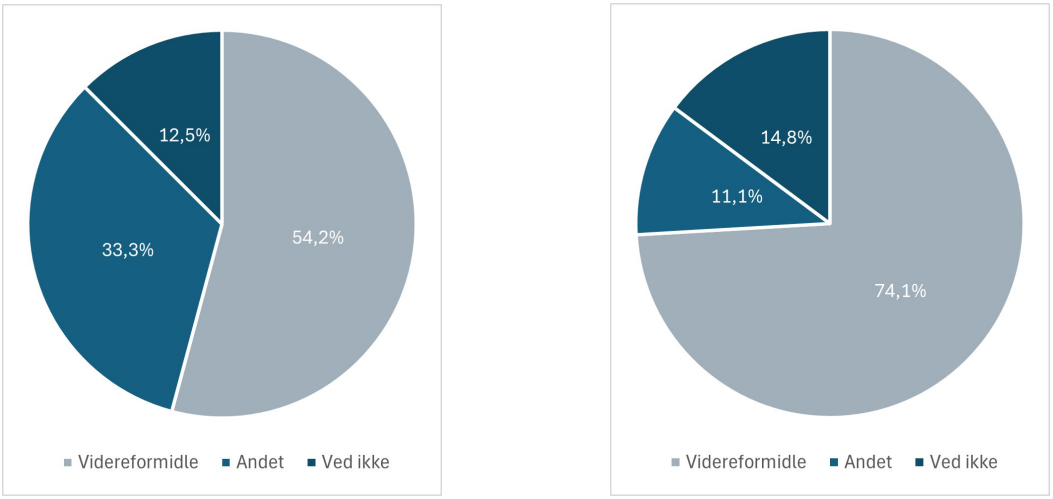
> *"(...) Uddannelsen har nærmest været en "cheat code"(...). Jeg havde ikke siddet hvor jeg var i dag, hvis jeg bare havde taget en IT-supporter uddannelse"* (Bilag [E4])

"Den har givet mig et helt nyt perspektiv på livet og hvad jeg gerne ville med det. Cyberen har introduceret mig til en masse super interessante mennesker (...). Alt i alt har det været et springbræt til den karriere jeg har nu" (Bilag [E4])

At cyberværnepligten har haft stor betydning, og været direkte afgørende for den videre karriere, er ikke kun isoleret til ovenstående udtaleser, men gennemgående for langt størstedelen af besvarelserne. Cyberværnepligten ses derfor som et springbræt, hvor tekniske personprofiler får et sikkerhedsperspektiv på cyberdomænet, og yderligere inddrages i relevant netværk indenfor feltet.

5.1.3 Ambassadørforståelse

De nuværende og tidligere cyberværnepligtige bedes i spørgeskemaet beskrive deres opfattelse af en god ambassadør for cybersikkerhed. Heraf fremkommer tre primære besvarelsestyper: En person, som forstår at videreformidle, budbringe, eller lære andre om god cybersikkerhed (Videreformidle); en person som er engageret (Andet); besvarelsen "ved ikke"(ved ikke). Vægtningen imellem de tre besvarelser for hhv. nuværende og tidligere cyberværnepligtige fremgår af figur 5.8a og 5.8b



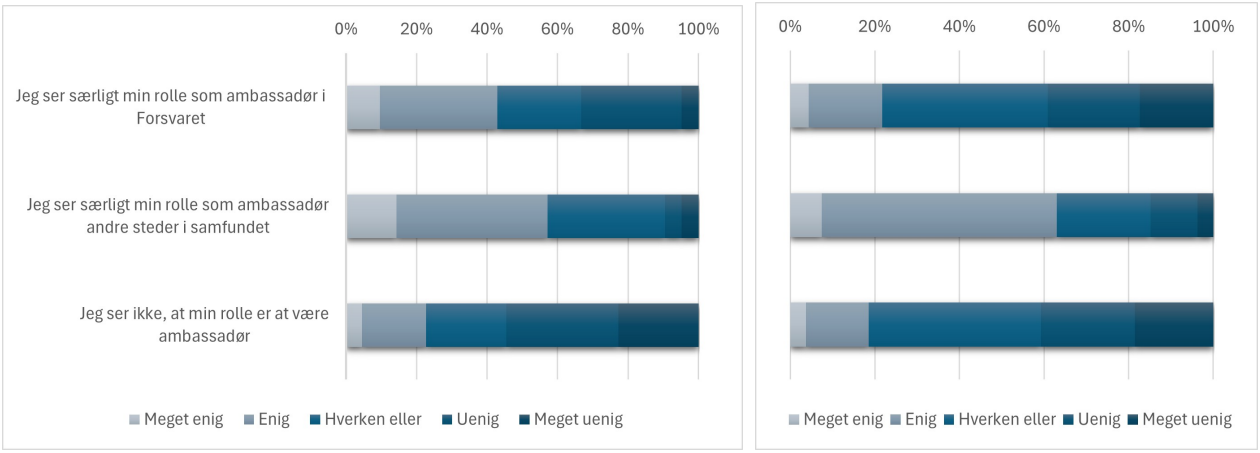
(a) Nuværende (b) Tidligere

Figur 5.8: Ambassadørforståelse for cyberværnepligtige

Det fremgår af dataen, at de cyberværnepligtige i overvejende grad forstår ambassadørrollen som en person der videreformidler, budbringer, eller lærer andre om god cybersikkerhed. Denne forståelse bekræftes i klyngeinterviewet af hold 7, der beskriver en ambassadør, som en budbringer for god sikkerhedskultur. Dog nævnes det også, at ambassadørrollen ikke nødvendigvis ses som en der står på en "piedestal", men i stedet en person, som selv har sunde vaner og derigennem er budbringer for god sikkerhedskultur.

Forståelsen for rollen som ambassadør vurderes også at have udviklet sig efter endt uddannelse, idet 54% af de nuværende cyberværnepligtige svarer "Videreformidle"og 33% svarer "andet", hvor 74% af de tidligere cyberværnepligtige svarer "Videreformidle"og kun 11% svarer "andet". Dette peger i retningen af, at forståelsen for rollen som ambassadør også stammer andre steder fra, hvilket bekræftes af udtalelser fra hold 7 i klyngeinterviewet. Her udtales det, at de er klar over, at rollen som ambassadør er en del af uddannelsen, men at det ikke opleves i dagligdagen.

Der ses også en udvikling i, hvor de cyberværnepligtige primært opfatter deres rolle som ambassadør, hvilket fremgår af figur 5.9a og 5.9b.



(a) Nuværende

(b) Tidligere

Figur 5.9: Ambassadørforståelse i samfundet

I figuren fremgår det, at godt 40% af de nuværende cyberværnepligtige er enige eller meget enige i, at rollen som ambassadør ses i Forsvaret, imens kun godt 20% af de tidligere cyberværnepligtige svarer enig eller meget enig til samme spørgsmål. Denne udvikling bemærkes særligt, eftersom uddannelsesbeskrivelsen, som ses i bilag [G3], har fokus på rollen som ambassadør for cybersikkerhed både i Forsvaret og i det civile.

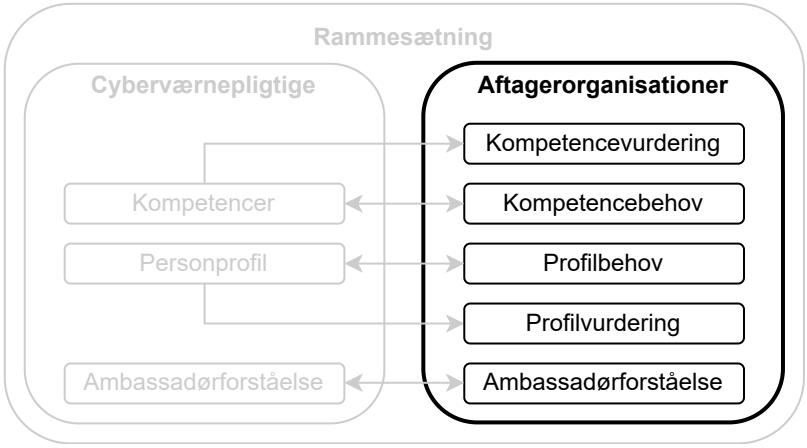
5.1.4 Opsummering

Undertema	**Centrale pointer**	**Uddybning**
Tekniske kompetencer	Netværkteori, Server, Red/Blue teaming, Generel IT-sikkerhed, certificeringer, hacking	- Gennemgående teknisk kompetenceprofil med særligt fokus på netværksteori
Organisatoriske kompetencer	Samarbejde, dokumentation, kommunikation, site battles, udvikling, frameworks	- Særligt fokus på samarbejde: Gode til rolle- & ansvarsfordeling, gode holdspillere
Ledelsesmæssige kompetencer	Governance, risikostyring, compliance, teamwork, ledelse, disciplin og processer	- Manglende kompetencer til selvstændig koordinering og strategi - Uddannelsen bidrager med få til ingen ledelsesmæssige kompetencer
Kompetencer generelt	Forskel på nuværende & tidligere CVPL'ere	- Tidligere CVPL'ere forstår bedre deres egne tekniske kompetencer end de nuværende
Profil	Analytisk, motiveret & drevet, samarbejdsvillige, beslutsomme, selvstændige, men uerfarne	- Motivation fra teknisk interesse - Militær som engangsoplevelse; birolle for motivation - Selvstændige, men brug for styring under pres - Samarbejdende og glade for CVPL-netværket
Ambassadørforståelse	Forskel fra nuværende og tidligere Ambassadør som én der videreformidler	- Nuværende CVPL'ere ser ambassadørrollen i Forsvaret i større grad end tidligere CVPL'ere - Forståelsen af en ambassadør som videreformidler er større hos tidligere end nuværende, hvor "andet"bliver mindre

Tabel 5.1: Centrale pointer og uddybning fra 'Cyberværnepligtige'

5.2 Aftagerorganisationer

I dette afsnit analyseres empirien fra aftagerorganisationerne, hvor der rettes fokus mod kompetence- og profilvurdering, egne kompetence- og profilbehov, samt ambassadørforståelse, som vist i figur 5.10.



Figur 5.10: Undersøgelsesdesign - Aftagerorganisationer

Empirien fra aftagerne består primært af de kvalitative interviews, der suppleres med kvantitative spørgeskemabesvarelser, som beskrevet i afsnit 3.5. Hensigten hermed er at lade de kvalitative interviews være styrende for at danne dybere indsigter, hvor den kvantitative data bruges supplerende. Fra behandlingen af de kvalitative data beskrevet i afsnit 3.6.1 *(Kodning af kvalitativ data)*, uddrages de temaer fra interviewene, som findes mest centrale for besvarelse af undersøgelsesspørgsmålene. De analyserede temaer, som ikke direkte besvarer undersøgelsesspørgsmålene, findes i bilag [H1].

5.2.1 Vurdering af cyberværnepligten

I dette afsnit vurderes cyberværnepligten fra aftagerorganisationer, hvilket bidrager til at besvare underspørgsmål 1. Vurderingen består, jf. afsnit 1.3 *(Undersøgelsesdesign)*, af en kompetence- og profilvurdering. Ydermere vurderes de cyberværnepligtiges bidrag i organisationen, samt evt. mangler og forbedringsmuligheder ved uddannelsen.

Kompetencevurdering

De cyberværnepligtige udmærker sig ved at have en bred vifte af kompetencer, der gør dem anvendelige på flere områder. Her fremhæves deres viden indenfor flere forskellige områder, f.eks. threat hunting, red teaming, blue teaming, osv. Især de cyberværnepligtiges tekniske kompetencer fremhæves. Det er vigtigt i junior-stillingerne, at der er teknisk forståelse, da det primært er indenfor det tekniske domæne deres jobfunktion ligger (IP 5):

"Vi er blevet imponeret over de tekniske kompetencer, som de cyberværnepligtige kommer med. De har præsteret på et væsentligt højere niveau, rent teknisk end vi egentligt havde forventet."(IP 9)

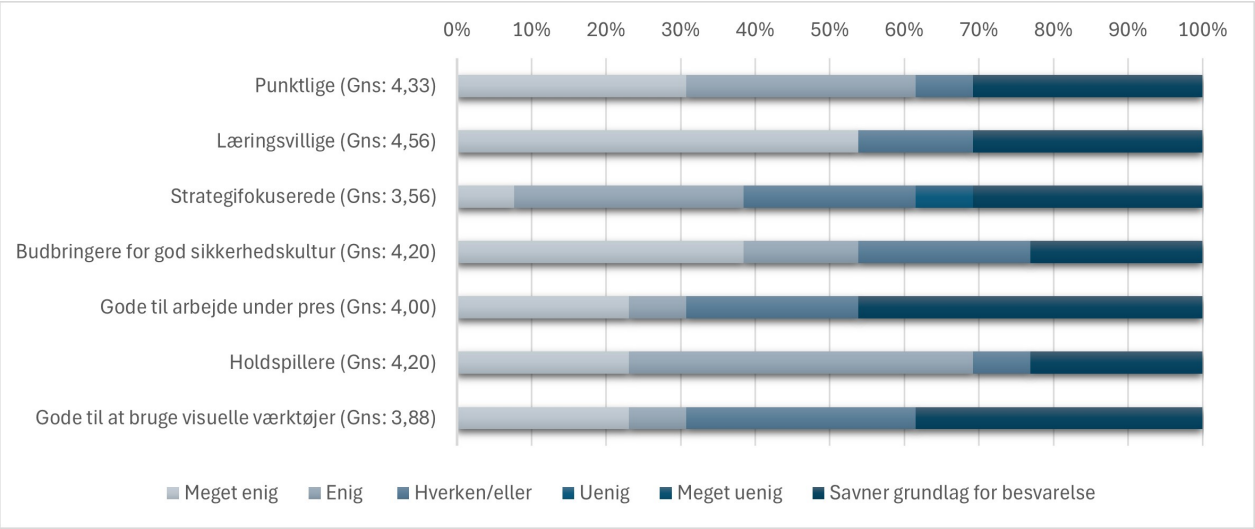
De cyberværnepligtige uddannes til et teknisk niveau der gør, at de kan varetage opgaver, der er langt over det forventede og hvad man kan forvente fra tilsvarende uddannelsesniveau (IP 9). Pointen understøttes af kvantitativ data, hvor 62% af aftagerne har svaret, at tekniske opgaver er de hyppigste iblandt cyberværnepligtige (bilag [E6]). Derudover har de cyberværnepligtige organisationsforståelse, samt er gode til at kommunikere (IP 5, IP 4). Den organisatoriske forståelse kommer de cyberværnepligtige til fordel i især større organisationer, hvor organisationsforståelse er vigtig. Dog nedprioriteres deres ledelsesmæssige kompetencer, da disse ikke ses relevante i forhold til de opgaver de varetager (IP 5).

Profilvurdering

De cyberværnepligtige omtales som nysgerrige, og har lysten og evnen til at sætte sig yderligere ind i ting og grave dybere. De har i forbindelse hermed en god evne til at studere og tilegne sig viden, der gør at de kan sætte tingene i perspektiv (IP 9, IP 8, IP 5, IP 6 og IP 10). Nysgerrigheden giver evnen til at lære mere og nå dybere niveauer, hvilket gør, at de kan udvikle sig indenfor cyberdomænet (IP 8).
Cyberværnepligtige omtales som omstillingsparate og lærenemme. De kan hurtigt flyttes fra én kontekst til en anden, og har let ved at tillære sig ny viden. Deres fundament gør, at der let og hurtigt kan bygges videre på deres viden. Det betyder i praksis, at de kan være bredt anvendelige og agere i stillinger, der egentlig ikke normalt anvendes som juniorstillinger (IP 5). Et unikt eksempel herpå er en cyberværnepligtig i en organisation med 25.000 ansatte, hvor denne anvendes som en del af kernen i et sikkerhedsteam (IP 5):

"Så på trods af en hel, hel ung junior profil, (...) endte han faktisk med at være en del af kernen i teamet, der ligesom bandt det hele sammen og kunne være med til at udvikle og tage nye udfordringer og flytte os." (IP 5)

Læringsevnen fremgår også i den kvantitative data, hvor der er enighed om, at de cyberværnepligtige er læringsvillige (gns: 4,00), som vist i figur 5.11. Ydermere opleves de cyberværnepligtige også særligt som *punktlige*, *budbringere for god sikkerhedskultur* og *holdspillere*.



Figur 5.11: Vurdering af cyberværnepligtige: De cyberværnepligtige opleves som...

De cyberværnepligtige omtales ofte som initiativrige, og selvstændigt tager ansvar for egne opgaver. De har desuden et fællesskab om cyberdomænet, som sandsynligt stammer fra cyberværnepligten (IP 9 og IP 10). På tværs af interview italesættes interesse for cyberdomænet som et kendetegn for de cyberværnepligtige. Det er tydeligt, at de brænder for det de laver (IP 9), og at de har fået vækket en essentiel interesse indenfor cyberområdet (IP 4):

> *"(...) fokuseret i virkeligheden, en mere fokuseret interesse, så det er måske i virkeligheden det, som har været den største forskel. Det er, hvis jeg får en risiko manager ind, så har de overhovedet ikke hørt om cyber. Men måske de synes, det er lidt interessant, hvorimod en værnepligtig har været... har en mere fokuseret interesse for domænet."* (IP 4)

Som citatet viser, kommer interessen til udtryk ved, at de er tændte på området (IP 4), at de videreuddanner sig (IP 8, IP 4, IP 6) og at de leverer kvalitet i det arbejde de foretager sig (IP 6). Deres interesse er mere fokuseret end andre sammenlignelige ansatte (IP 4).

Militær baggrund

Vedrørende de cyberværnepligtiges militære baggrund, fremgår to tendenser. På den ene side spiller deres militære baggrund ikke nogen fremtrædende rolle i forhold til deres profil (IP 7, IP 5). Omvendt italesættes den militære baggrund som noget positivt der har styrket de cyberværnepligtiges personprofil (IP 6, IP 4, IP 8). Hertil nævnes, at den militære baggrund har skabt disciplinerede og motiverede profiler (IP 4, IP 6) med en ansvarlig og positiv attitude (IP 6).

Vurdering af cyberværnepligtiges bidrag

Gennemgående for interviewpersonerne er, at de cyberværnepligtige formår at opnå et passende kompromis mellem kompetenceniveau og uddannelseslængde. De uddannes på et godt grundniveau uden at være overkvalificerede (IP 5). De cyberværnepligtige kommer med en teknisk baggrund, der gør dem i stand til at arbejde sammen med etablerede teknikere:

> *"(...) har jeg ikke indtrykket af, at den faglærte, føler den cyberværnepligtige er på slæb (...) De ved godt hvad det er, det handler om. Så vi starter ikke fra bunden af."* (IP 9).

De er fagligt funderet og gør det godt selvstændigt (IP 9, IP 6). De cyberværnepligtige passer godt ind i juniorstillinger, f.eks. i en SOC-funktion. Dette supporteres i de kvantitative besvarelser, hvor den stilling, som de cyberværnepligtige hyppigst besidder er SOC-relaterede stillinger (5 besvarelser) og juniorstillinger (3 besvarelser). Hertil er kurser, certificeringer eller oplæring hos aftagerorganisationen medvirkende til at bygge videre på de grundlæggende kompetencer fra cyberværnepligtsuddannelsen. Deres attitude og vilje til at udvikle sig gør dem eftertragtede og hurtige at inkorporere (IP 8, IP 6).

Mangler og forbedringsmuligheder

En enkelt interviewperson nævner mangel på praktiske erfaringer og driftskompetencer (IP 4). Hertil kommer mulighed for forlængelse af uddannelsen igennem en praktikperiode, der fordelagtigt vil kunne foregå i civile aftageres driftsorganisation (IP 4). Ligeledes nævner flere interviewpersoner, at de oplever mangel på specifikke områder, f.eks. specifikke teknologier såsom cloud, bring-your-own-device og endpoint (IP 6, IP 9, IP 4), men også ikke-tekniske områder som f.eks. forretningsforståelse (IP 6). Manglende formel uddannelse nævnes som en problemstilling. Det vil sige ansættelse af de cyberværnepligtige som de facto ufaglærte i faglærte stillinger, og ligeledes mulighederne for at opkvalificere de cyberværnepligtige internt i Forsvaret (IP 9, IP 8).

I Forsvaret ses et behov for en slags cyberværnepligtig på både konstabel-, befalingsmands- og officersniveau. Der er behov for at have en karrierevej på alle niveauer (IP 9). Det er naturligt, da cyber udspiller sig på alle niveauer, og det er en kompetence der bør haves in-house (IP 9). Dette giver også mulighed for flere indgange til private aftagerorganisationer på tværs af uddannelsesniveau.

5.2.2 Opsummering - vurdering af cyberværnepligten af aftagere

I tabel 5.2 opsummeres de væsentligste pointer ift. aftagernes vurdering af de cyberværnepligtige.

Undertema	**Centrale pointer**	**Uddybning**
Kompetence-vurdering	Bred kompetencevifte: Tekniske kompetencer, kommunikation og organisatorisk forståelse, manglende ledelse	- Kompetenceprofilen matcher en typiske jobfunktion i større organisationer, hvor ledelse varetages af andet personale - CVPL's tekniske kompetencer har hovedfokus
Profilvurdering	Læringsvillige- og nemme, punktlige, holdspillere	- Særligt fremtrædende er de cyberværnepligtiges evne til at tilegne sig ny viden - Fokuseret kompetenceprofil medfører, at de udvikler og videreuddanner sig indenfor domænet
Militær baggrund	Todeling: Ingen mærkbar effekt Bidrager positivt til profilen	- Den miltitære baggrund giver ingen mærkbar forskel for CVPL - Den militære baggrund bidrager til at skabe disciplinerede, ansvarlige og motiverede profiler
Vurdering af cyberværnepligtiges bidrag	Starter ikke fra bunden Godt grundniveau Vilje til udvikling, fagligt funderet	- CVPL har et grundniveau, som medfører, at de hurtigt kan indgå i samarbejde med etablerede teknikere i juniorstillinger i f.eks. en SOC-funktion
Mangler og forbedrings-muligheder	Manglende på: Praktisk erfaring, driftskompetencer og specifikke teknologier Cyberuddannelse på flere niveauer	- Forlængelse af uddanelsen igennem praktikperiode med fokus på drift - Uddannelse af Cyber-officer, cyber-konstabel og cyber-befalingsmand

Tabel 5.2: Pointer fra afsnit omhandlende 'Vurdering af cyberværnepligten' i aftagerorganisationer

5.2.3 Behov hos aftagerorganisationer

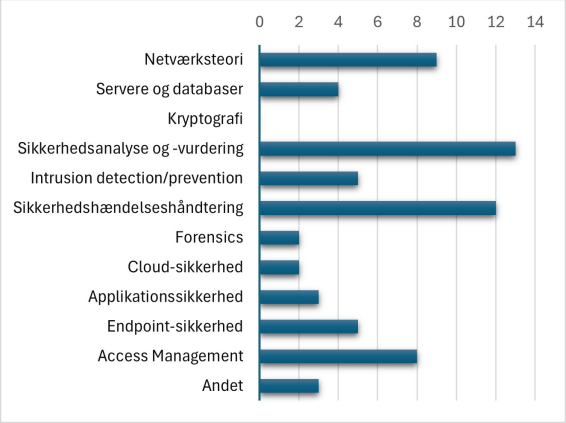
I dette afsnit analyseres de behov, som aftagerorganisationerne har for at opbygge god cybersikkerhed, hvilket bidrager til at besvare underspørgsmål 2. Afsnittet inddeles efter kompetence- og profilbehov, hvor antallet af cyberværnepligtige slutteligt adresseres.

Kompetencebehov

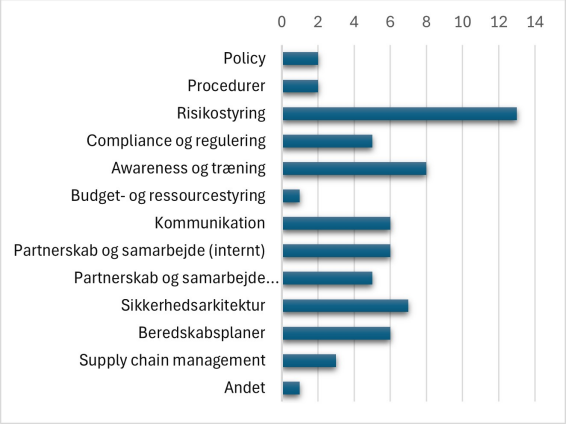
Aftagernes kompetencebehov er primært bestående af tekniske kompetencer, hvor særligt forståelse for netværk, servere, protokoller og kommunikation fremhæves (IP 9, IP 10, IP 5, IP 7). Dette stemmer overens med kvantitative data som viser, at netværk er den 3. mest udvalgte tekniske kompetence (9/15). Den mest efterspurgte tekniske kompetence er dog sikkerhedsanalyse- og vurdering, efterfulgt af sikkerhedshændelseshåndtering, hvilket ikke kommer til udtryk i den kvalitative data.

Indenfor det organisatoriske domæne, fremhæves i kvalitative data særligt behov for kompetencer indenfor regulativer såsom ISO og NIS2 (IP 9, IP 4, IP 6), men også en gennemgående forståelse for organisationen og kommunikation er fremtrædende hos interviewpersonerne (IP 8, IP 4). Dette står i kontrast til spørgeskemaundersøgelsen, hvor risikostyring (13/15), awareness og træning (8/15), samt sikkerhedsarkitektur (7/15) udvælges som værende mest centrale.

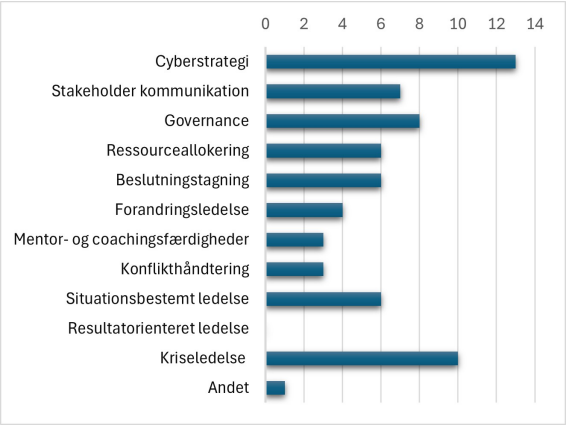
Indenfor det ledelsesmæssige område, er det primært kompetencebehov indenfor governance, risk management og compliance (IP 6, IP 10, IP 9), der fremhæves som centrale. Dette understreger, at risikostyring anses som værende vigtigt indenfor både det organisatoriske og ledelsesmæssige domæne. Ydermere er de mest udprægede ledelsesmæssige kompetencer i den kvantitative data; cyberstrategi (13/15), kriseledelse (10/15), governance (8/15) og stakeholder kommunikation (7/15), hvilket understreger, at governance og risikostyring er et gennemgående tema i både den kvantitative og kvalitative data.



Figur 5.12: Figure A: Tekniske kompetencer



Figur 5.13: Figure B: Org. kompetencer

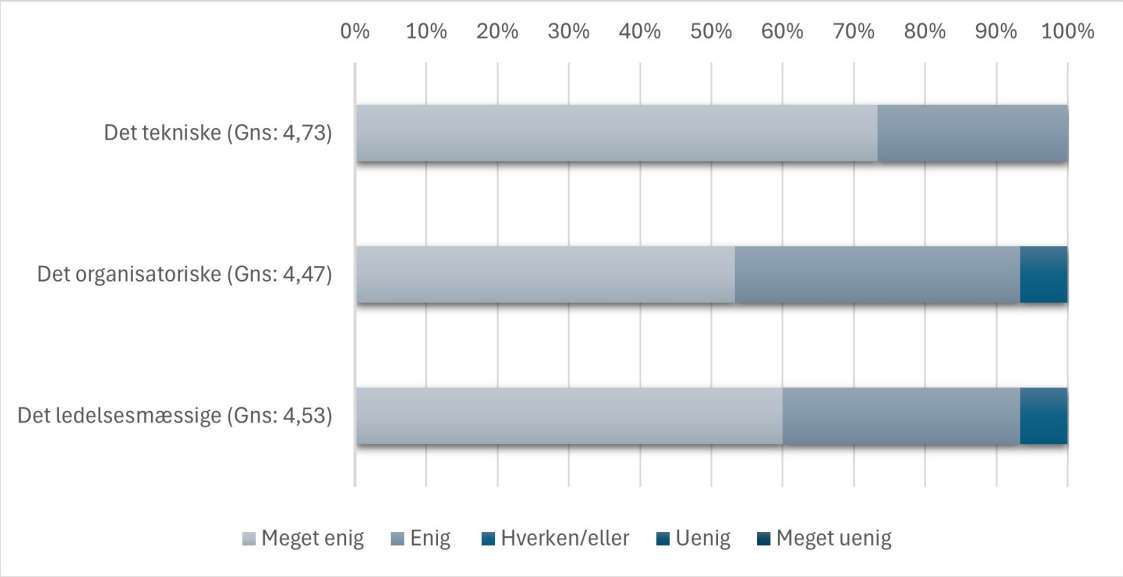


Figur 5.14: Figure C: Ledelses kompetencer

Generelt er der iblandt interviewpersonerne konsensus om, at en grundlæggende forståelse for det tekniske domæne er nødvendig i arbejdet med cybersikkerhed, men samtidigt også, at en bredere vifte af kompetencer er nødvendige for at opbygge cybersikkerhed, hvilket udtrykkes:

> *"Der er brug for nogle, der er meget stærke teknisk, der er brug for nogle, der kan kommunikere, der er brug for nogle, der har et blik for det organisatoriske og for governance, risk and compliance."(IP 10)*

Dette kommer i nogen grad til udtryk i den kvantitative data, hvor de tekniske kompetencer vurderes af større betydning for opbygning af cybersikkerhed, som vist i figur 5.15. Dog er både organisatoriske og ledelsesmæssige kompetencer vurderet marginalt lavere, hvilket understreger, at kompetencer indenfor alle tre domæner er nødvendige.



Figur 5.15: Aftagernes vægtning mellem tekniske, organisatoriske og ledelsesmæssige kompetencer

Profilbehov

Den hyppigst omtalte profil er en teknisk profil, der har sans for detaljer og er analytisk af natur. Én aftager nævner, at det ikke er muligt for alle at løse tekniske opgaver, men at næsten hvem som helst kan løse opgaver indenfor f.eks. governance (IP 9). Denne holdning anses dog ikke som gennemgående, eftersom flere af aftagerne nævner, at det ikke er en specifik profiltype som skaber kvalitet i arbejdet med cybersikkerhed, men i stedet en bred vifte af forskellige profiler. Ydermere nævner flere, at det i ligeså høj grad er motivationen og mindsettet, som er i fokus, når den rette kandidat til en stilling udvælges (IP 8, IP 6, IP 4). Det kommer f.eks. til udtryk på følgende måde:

> *"vi kigger rigtig meget på, at man har et helt naturlig drive og motivation omkring det her, fordi det er et et marked, der aldrig stopper"(IP 7)*

Netop motivation og drive italesættes som en kvalitet ved de cyberværnepligtige i afsnit 5.2.1 *(Vurdering af cyberværnepligten)*.

Antal af cyberværnepligtige

Der er generel konsensus om, at antallet på 32 cyberværnepligtige pr. år vurderes som værende for lavt i forhold til det behov og de aftagermuligheder, der er i samfundet (IP 9, IP 4, IP 5, IP 6, IP 7). Det vurderes ydermere af én aftager, at den største udfordring ved cyberværnepligten netop er, at antallet er tilpas lavt (IP 6):

> *"Få nu fingeren ud, og så få allokeret nogle flere værnepligtige". (...) Jeg kan ikke få nok! Og det er ikke mig, der ikke kan få nok, vi kan ikke få nok i det her land. Det kan vi sgu ikke!" (IP 6)*

Der ses et potentiale i at uddanne langt flere cyberværnepligtige, men der erkendes samtidigt, at der skal være mulighed for at kunne afsætte dem på en meningsfuld måde (IP 4, IP 9). En fortsættelse i Forsvaret ville kræve en form for cyber-karrierevej, eller at der fandtes en slags cyber-elev stilling (IP 4). Et alternativt perspektiv er, at flere cyberværnepligtige fører til en øget talentmasse, der kan videreuddannes (IP 10). Et modsatrettet perspektiv hertil er, at der hellere uddannes 32 cyberværnepligtige pr. år med den nuværende kvalitet fremfor en øget volumen (IP 8). Her ses det tvivlsomt, hvorvidt volumen kan øges uden at gå på kompromis med kvaliteten, og det er netop kvaliteten i cyberværnepligten, som vurderes vigtig for deres effektivitet (IP 8).

5.2.4 Opsummering - kompetencebehov hos aftagere

I tabel 5.3 ses en opsummering af de væsentligste kompetencebehov hos aftagerne.

Undertema	**Centrale pointer**	**Uddybning**
Kompetence-behov	Netværksforståelse, sikkerhedsanalyse, hændelseshåndtering Organisations- og framework-forståelse, risikostyring, awareness GRC, cyberstrategi, kriseledelse	- Forståelse for det tekniske domæne er forudsætningen for cybersikkerhed - Samtidigt er en bred vifte af kompetencer på tværs af alle domæner nødvendig
Profilbehov	Teknisk, analytisk profil Sans for detaljer	- Behov for en bred vifte af profiler - Motivation og mindset er afgørende
Antal af cyber-værnepligtige	Antallet er kraftigt under behov Flere uddannet CVPL kræver nye strukturer	- Behovet hos aftagerne er endnu ikke afdækket - Det er nødvendigt at kunne opretholde kvaliteten, og at kunne afsætte dem meningsfuldt, ved skalering af CVPL

Tabel 5.3: Pointer fra afsnit omhandlende 'Behov hos aftagerorganisationer'

5.2.5 Ambassadørrollen

I dette afsnit analyseres aftagerorganisationernes perspektiver på ambassadørrollen, hvilket bidrager til besvarelse af underspørgsmål 3 i analyse del 2.

Ambassadørforståelse hos aftagerorganisationer

En ambassadør for cybersikkerhed skal besidde evnen til at påvirke kollegaers awareness, samt være motiveret og drevet til at skabe årvågenhed omkring cyber og øge cyberhygiejnen i organisationen (IP 10, IP 7). Ambassadøren skal være brobygger imellem den tekniske- og ikke-tekniske verden og det kan ske ved hjælp af værktøjer, som awareness-træning og dialog (IP 9, IP 5, IP 7). Der er generelt et positivt syn på konceptet omkring ambassadørrollen.

Aftagerorganisationers vurdering af cyberværnepligtiges ambassadørrolle

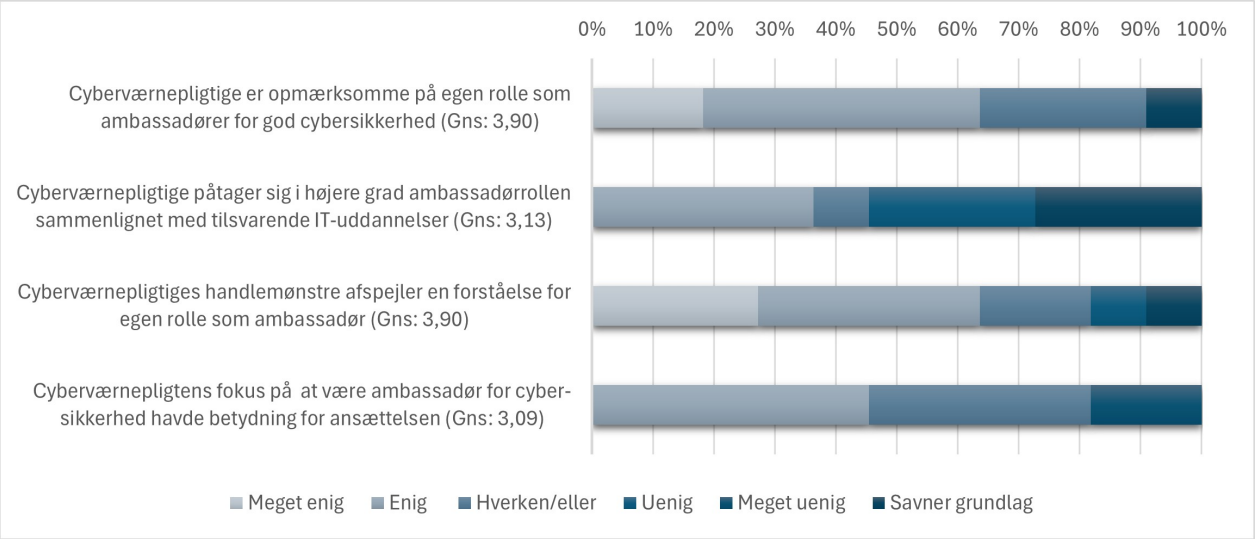
Flere af aftagerne nævner, at ambassadørrollen ikke er noget de har lagt mærke til hos de cyberværnepligtige:

> *"det er der ikke noget, jeg har oplevet i en cyberværnepligtig, hvor de kommer et sted hen og jeg tænker, der er sgu noget mindset-mæssigt eller proaktivitet (...). Overhovedet ikke"(IP 7)*

Det suppleres med, at det kan være svært at påtage sig en sådan rolle efter 6 måneders uddannelse (IP 9, IP 4, IP 7). Ligeledes kommer konteksten også på spil her, da nogle af de cyberværnepligtige er ansat i roller, hvor det at agere ambassadør ikke giver mening (IP 4, IP 8, IP 5). Yderligere nuanceres cyberværnepligtige i ambassadørrollen som et HR-initiativ, hvor den virkelige ønskede effekt af cyberværnepligtige er teknisk kompetence:

> *"Ja, det er jo crap. Det er jo spild af kompetente menneskers tid, altså at få en eller anden langhåret Sofie fra marketing til at lave det der, altså det ved jeg godt, det giver jeg ikke en skid for. Lad os nu få nogle hardcore folk som forstår teknik, som kan forstå risikovurdering og andet"(IP 6)*

I modsætning til ovenstående, kommer det i den kvantitative data til udtryk, at de cyberværnepligtige i nogen grad er opmærksomme på egen rolle som ambassadør, samt at de cyberværnepligtiges handlemønstre afspejler en forståelse for rollen (Gns: 3,9 & 3,9), som vist i figur 5.16.



Figur 5.16: Aftageres vurdering af cyberværnepligtiges rolle som ambassadør

De aftagere, som har bemærket de cyberværnepligtige agere ambassadører, beskriver det meget kontekstbestemt, samt at kræve den rigtige setting (IP 9). Et andet perspektiv er, at ambassadørrollen italesættes som et *netværk*. Her fokuseres på, at de cyberværnepligtige bibeholder kontakten til deres netværk fra Forsvaret (IP 8). I dette netværksperspektiv, er ambassadørforståelsen en metode til at dele viden (IP 8). Dette netværk udvides igennem både uddannelse og cyberevents, hvor de kan påvirke andre unge og personer med samme interesse (IP 10).

Ambassadørrollen hos de cyberværnepligtige vurderes dog ikke mere fremtrædende end hos tilsvarende IT-uddannelser (Gns: 3,1), og ambassadørrollen vurderes ligeledes ikke afgørende for ansættelsen (Gns: 3,1). Ambassadørforståelsen er derved ikke unik for de cyberværnepligtige, og kan derfor ikke tilskrives uddannelsen isoleret set.

5.2.6 Opsummering - ambassadørforståelse hos aftagere

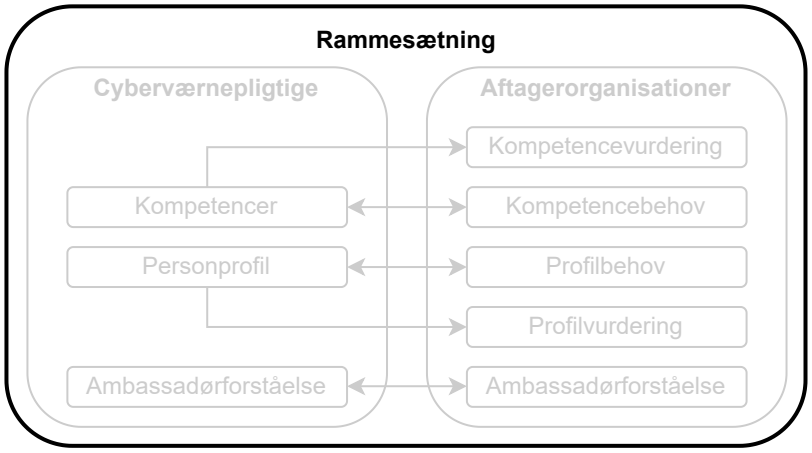
I tabel 5.4 opsummeres de væsentligste pointer ift. aftagernes forståelse for ambassadørrollen.

Undertema	Centrale pointer	Uddybning
Ambassadør-forståelse hos aftager-organisationer	Påvirker kollegaers awareness positivt Brobygger mellem ikke-teknisk og teknisk	- En ambassadør skal kunne bidrage til kollegaers årvågenhed ift. cyberhygiejne ved at bygge på til den tekniske verden på forståelig vis
Aftager-organisationers vurdering af cyberværne-pligtiges ambassadørrolle	Kommer generelt ikke aftagerne Rollen kommer til udtryk på andre måder, eks. gennem netværk og interesse Rollen har ikke betydning for ansættelsen	- Svært at påtage sig et sådant ansvar efter 6 måneders uddannelse - Deres interesse smitter af på andre unge ved cyberevents og uddannelse - Ofte ansat i jobfunktioner, hvor det ikke er muligt at påtage sig ambassadørrollen

Tabel 5.4: Ambassadørforståelse hos aftagere

5.3 Rammesættende interessenter

I dette afsnit analyseres empirien fra de rammesættende interessenter, som vist i figur 5.17.



Figur 5.17: Undersøgelsesdesign - Rammesættende interessenter

Empirien består af kvalitative interviews, der anvendes til at danne indsigter fra rammesættende interessenter. Afsnittets fund er baseret på fremgangsmåde i afsnit 3.6.1. Perspektiverne indgår ikke direkte i besvarelsen af underspørgsmålene, men bruges understøttende/nuancerende i besvarelsen af problemformuleringen fra myndighedsniveau. De analyserede temaer, som ikke direkte relateres til undersøgelsesspørgsmålene, findes i bilag [H1].

5.3.1 National cyberindsats

I dette afsnit fremsættes de tre rammesættende interessenters perspektiver på den nationale cyberindsats.

Cyber og uddannelse

Der er generelt et stort behov for folk indenfor cyberområdet, og især de tekniske folk nævnes (IP 2). Dog skal der også tænkes alternative veje til de formelle cyber-uddannelser, så folk med baggrund i f.eks. processer eller risikostyring også kan arbejde med cyber (IP 2). Det er vigtigt, at indsatsen startes og interesse fanges allerede i folkeskolen, så der er en endnu større og bredere talentmasse (IP 2).

> *"Vi kan ikke nøjes med kun at kigge på, hvor mange bachelorer laver vi inden for cybersikkerhed. Nej, Vi er nødt til at tænke meget bredere. Får vi stimuleret nok nede i folkeskolen, får vi skabt interessen op igennem ungdomsuddannelserne?"* (IP 2).

Cyberværnepligtsindsatsen er en blandt flere indsatser, og det er nødvendig med flere forskellige typer indsatser for at få nok opmærksomhed på området (IP 2, IP 3).

Ambitioner for cyberområdet

Der er konsensus om, at cyberindsatsen bør prioriteres, og at det nationale cyber-niveau bør stige. Dette kan ske gennem samarbejde, regulativer, kapaciteter og selve oparbejdningen af disse. Samarbejde skal både ske på tværs af landegrænser og mellem sektorer, så viden og erfaring kan vandrer og akkumuleres (IP 2). Sammenlignet med andre nationer, er der i Danmark forbedringsrum, når det kommer til at arbejde sammen på tværs af sektorer indenfor cyber (IP 2). Måden hvorpå cyberniveauet i Danmark kan opnå et bedre samarbejde og ensretning er bl.a. gennem regulativer som NIS2, hvor der lægges vægt på, at EU med NIS2 opprioriterer vidensdeling på tværs af sektorer, nationalt og internationalt (IP 2). Dertil påpeges, at rammeforliget 2024-2033 fokuserer på at prioritere styrkelsen af cyberforsvar (IP 3). Det fremgår af disse udtalelser, at der er fokus på cyber fra politisk niveau. Dog fremhæves, at der er kan forekomme oversættelsesproblematikker fra politiske ambitioner til operationaliering og tiltag, når viften af cybertrulser er bred (IP 1).

CFCS som IT-sikkerhedsmyndighed

Det fremgår, at sektoransvarsprincippet har en stor betydning for, hvorfor CFCS arbejder og rådgiver som de gør. I dag varetager forskellige sektorer selv ansvaret for at opbygge cybersikkerhed, hvortil CFCS som myndighed har en rådgivende rolle frem for en håndterende (IP 2, IP 3). Hertil problematiseres sektorernes evne til at arbejde hensigtsmæssigt sammen (IP 2), når CFCS er underlagt FE, og derfor ikke umiddelbart må videregive information på tværs af sektorer. Dog hævdes det, at CFCS er den oplagte kandidat til at spille sektorerne økosystemet sammen, men samtidigt erkendes det, at der er plads til forbedring (IP 2). Det kan f.eks. være problematisk at inkludere SMV'erne, eftersom dette ikke er CFCS' fokus, men derimod Erhvervs- eller Digitaliseringsstyrelsens (IP 2):

> *"Altså får man så koordineret godt nok på tværs, får man delt trusselsinformation eller sårbarheds information eller hvad det nu måtte være. Alt muligt cyberthreat intel på tværs godt nok, og der tror jeg, at svaret er, at der er room for improvement"* (IP 2).

Det tilføjes hertil, at de nationale cyberstrategier kan være med til at binde tingene bedre sammen, og dermed skabe denne røde tråd på tværs af sektorer (IP 2). Placeringen af CFCS under FE er en politisk beslutning, hvor det påpeges at tungt efterretningsbaseret arbejde ikke kan flyttes væk fra FE, men at selve vejledningsindsatsen og rådgivningsindsatsen i fremtiden kan placeres andetsteds (IP 3).

5.3.2 Opsummering - national cyberindsats

En opsummering af den nationale cyberindsats ses i figur 5.5.

Undertema	**Centrale pointer**	**Uddybning**
Cyber og uddannelse	Stort behov for medarbejdere indenfor cyber	- Vejen til en cyberuddannelse skal nytænkes for at imødekomme behovet
Ambitioner for cyberområdet	Nationalt og internationalt samarbejde Manglende retningslinjer for håndteringen af regulativer på det operationelle niveau	- Nationalt og internationalt samarbejde etableres gennem regulativer - Svært at operationalisere politiske tiltag
Cybertrusler	Cybertruslen er stor mod Danmark	- En holistisk indsats er nødvendig for at imødekomme truslerne
CFCS som IT-sikkerheds-myndighed	CFCS er placeret under FE Fokus på bredt samarbejde på tværs af sektorer Todeling i CFS	- Placeringen af CFCS under FE har besværliggjort samarbejde og evnen til at agere rådgivende instans - De nationale cyberstrategier skal sikre det brede samarbejde - Det foreslås at CFCS' rådgivningsindsats og efterretningsindsats separeres

Tabel 5.5: Pointer fra afsnit omhandlende 'National cyberindsats'

5.3.3 Cyberværnepligten

I dette afsnit fremsættes de rammesættende interessenters perspektiver på cyberværnepligten.

Uddannelse og evaluering

Uddannelsens indhold er sammensat hos FSR, og er derved ikke dikteret oppefra. Selve uddannelsens indhold godkendes formelt af Hærkommandoen, der løbende holdes orienteret om indhold og udvikling. Det sker i koordination med de andre to værn (Flyverkommandoen og søværnskommandoen), hvor indholdet indrapporteres til Forsvarskommandoens styregruppe for cyber (IP 1). Alle fag på uddannelsen bliver løbende evalueret internt af både instruktører og elever, og yderligere evalueres de enkelte hold. Ydermere har FSR fået feedback fra tidligere cyberværnepligtige i job. Den eksterne feedback omfatter desuden sparring med erhvervslivet ift. deres ønsker, behov og tendenser. Den eksterne feedback er primært sket i samarbejde med hjemmeværnets samtænkningssektion. Selve cyberværnepligtsuddannelsen er nødt til at være dynamisk, og følge den digitale udvikling i erhvervslivet, hvilket sker for løbende evaluering og feedback (IP 1). Den løbende evaluering sker i en national kontekst. Lignende uddannelser forekommer også i andre, allierede lande, men der er ikke bilateralt samarbejde for at evaluere cyberværnepligterne på tværs af lande (IP 1).
Særligt for uddannelsen italesættes vigtigheden af team og samarbejde. I Forsvaret vægtes enheden højere end individet, hvilket giver noget særligt:

> *"De arbejder i teams, de har forståelse for, at de arbejder i en større ramme, og kan agere i det. Det er jo noget vi kan i Forsvaret. Så den der teamwork og team spirit dér, det er virkelig noget de får med sig her."* (IP 1)

Det er vigtigt for Forsvaret, og en prioriteret del af uddannelsen, at de cyberværnepligtige bliver ambassadører for god cybersikkerhed (IP 1). Rollen italesættes som vigtig, og forstås som en formidler af god cybersikkerhed (IP 1). Det fremhæves, at det er en krævende opgave, der foregår både i tale og handling (IP 1). Dog påpeges det, at ambassadørrollen kun italesættes, og at der på uddannelsen ikke findes konkrete værktøjer eller andet, som understøtter rollen (IP 1). Det forventes implicit, at de cyberværnepligtige påtager sig rollen og agerer herefter. Ambassadørrollen opstår derved indirekte under uddannelsen. Det fremhæves, at ambassadørrollen er særlig for Forsvarets Cyberværnepligtsuddannelse, og ikke nødvendigvis afspejles i andre civile IT-sikkerhedsuddannelser (IP 1). Samtidigt erkendes det, at selve rollen og virket heri er individuel, og derfor også påvirkes af persontype (IP 1).

Ansættelsesbarrierer og fastholdelse for cyberværnepligtige

Det har været særligt problematisk at motivere cyberværnepligtige til ansættelse i hæren efter endt cyberværnepligt, da der opstilles et krav om gennemførsel af HRU. HRU er en uddannelse, der fjerner de cyberværnepligtige fra cyberdomænet i ca. 8 måneder, hvilket er blevet opfattet som en barriere for flere cyberværnepligtige (IP 1). Problemstillingen er knyttet til hæren, da dens soldater skal være sammenlignelige

på tværs. Dette sker på trods af, at andre kritiske funktioner som sygeplejersker, regnskabsførere mv. ikke står overfor samme krav og anvendes med supplerende uddannelse (IP 1). Det er især interessant i lyset af, at Hæren står overfor massive rekrutterings- og fastholdelsesudfordringer. Det har desuden været svært for FSR at placere cyberværnepligtige i reservestrukturen, da dens opstilling er kraftigt reduceret. I forlængelse heraf, er tilknytningen til Forsvaret efter cyberværnepligtsuddannelsen reduceret til et frivilligt netværk, samt en tilknytning til et netværk forankret i Hjemmeværnet (IP 1). Det snævre medarbejderperspektiv kritiseres bl.a. for manglende forståelse for hvad unge i dag forventer af Forsvaret som arbejdsplads, og der efterlyses en mere moderne tilgang med inspiration i det private (IP 2).

Et andet perspektiv på karrierevejen fremfører, at det selvfølgelig er op til den enkelte cyberværnepligtige, om vedkommende vil fortsætte i Forsvaret eller ej. Det er fint at nogle vil, men alternativt anvender de bare deres færdigheder i det civile (IP 2, IP 3), og det ligger stadigvæk indenfor målrammen for værnepligten at udfylde sin samfundspligt (IP 1). *"Det spiller en mindre betydning præcis, hvor de ender set i et større perspektiv, og derfor skal man nok egentlig bare være glad og stolt af, at så mange (40%) ender i Forsvaret."* (IP 2). Det tal er højt sammenlignet med almindelig værnepligt (IP 3). FSR ser gerne selv, at flere fastholdes i Forsvaret, eftersom mange er motiverede heraf, og at der desuden er brugt resourcer på at uddanne dem, men det er ikke et krav (IP 1). Fastholdelse af de cyberværnepligtige kræver dog en struktur de kan fastholdes i, og her har Forsvaret som organisation ikke været opgaven moden. Forholdet er især forbedret ved flyvevåbnets F-35 projekt, som absorberer en del cyberværnepligtige (IP 1).

Rolle på nationalt plan

Ifølge (IP 1, IP 2, IP 3) er de cyberværnepligtiges rolle på nationalt plan, at hjælpe med at mætte kompetencebehovet for cybersikkerhed i samfundet. Det fremhæves, at det er begrænset, hvor meget 32 cyberværnepligtige om året kan gøre, men at det giver en positiv effekt uanset hvad (IP 3). Det vurderes, at antallet af cyberværnepligtige kan øges, men det kræver politisk prioritering og justering af antallet af værnepligtige i værnepligtsloven (IP 1). Der har generelt været stor tilslutning til uddannelsen, og alle tidligere hold har været fyldt op. Det ses desuden, at når cyber er stort i samfundet, afspejles det i ansøgerantallet (IP 1). Det har ikke været svært at hverve motiverede kandidater til uddannelsen (IP 1). Antallet af cyberværnepligtige kan derfor bestemmes ud fra, hvorvidt de absorberes i samfundet. Dette må vurderes ud fra den effekt de skaber (IP 2). Ifølge interessenterne er det ikke afgørende, om de fortsætter i Forsvaret eller i det private efter uddannelsen, eftersom deres effekt stadig vil påvirke cyberniveauet i Danmark (IP 3, IP 1).

5.3.4 Opsummering - cyberværnepligten

Tabel 5.6 opsummerer de væsentligste fund.

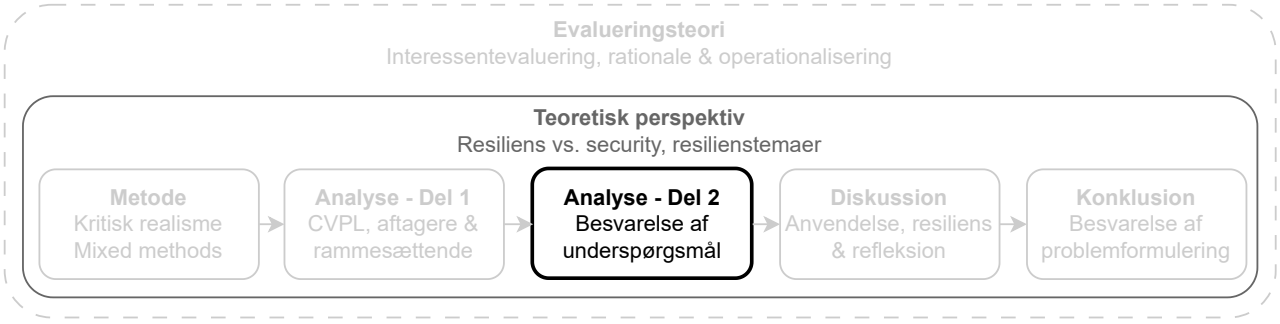
Undertema	**Centrale pointer**	**Uddybning**
Uddannelse og evaluering	Evaluering af uddannelsens indhold sker internt Ekstern samarbejdspartnere inddrages til evaluering Ambassadørrolle for CVPL	- Den interne evaluering har fokus på at udvikle uddannelsens faglige indhold - De eksterne består primært af hjemmeværnets samtænkningssektion samt tidligere cyberværnepligtige - Forsvaret ønsker at de er ambassadører på området, både direkte og indirekte
Ansættelsesbarriere og fastholdelse for cyberværnepligtige	Hæren oplever fastholdelsesproblematikker Kontakt til tidligere CVPL sker gennem frivilligt netværk	- Problematikkerne opstår, eftersom hæren kræver en HRU for ansættelse af CVPL - Uagtet hvor CVPL's kompetencer anvendes, opfattes det som positivt bidrag til den nationale sikkerhed
Rolle på nationalt plan	CVPL bidrager til at mætte kompetencebehovet på cyber	- Bidrager til at mætte behovet både indenfor det militære og civile

Tabel 5.6: Pointer fra afsnit omhandlende 'Cyberværnepligten'

Kapitel 6

Analyse - Del 2

Analysens del 2 har til formål at besvare underspørgsmålene, som vist i figur 6.1. Dette sker ved at sammenholde hovedfund fra analysens del 1 med det teoretiske perspektiv. De væsentligste pointer fra analyse del 1 fra hhv. de cyberværnepligtige, aftagere og rammesættende enheder ses opsummeret i tabel 5.1, 5.2, 5.5 og 5.6, og de teoretiske perspektiver ses i kapitel 2. Inddragelse af det teoretiske perspektiv sker m.h.p. at tilgå det dybe forståelsesstratum, hvilket er et hovedtræk i den *kritiske realisme* beskrevet i afsnit 3.1 *(Videnskabsteori)*.



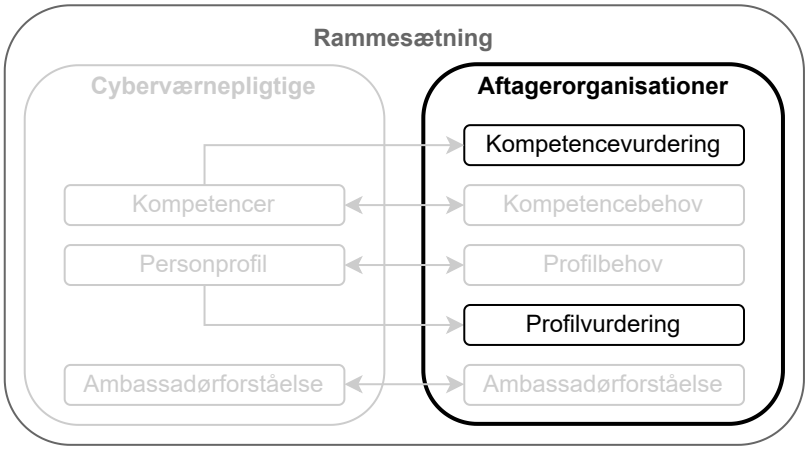
Figur 6.1: Analyse del 2 i undersøgelsesstrukturen

6.1 Vurdering af cyberværnepligtige

Dette afsnit har til formål at besvare underspørgsmål 1, som lyder:

Hvordan vurderes cyberværnepligtiges kompetencer og personlige profil af aftagerorganisationer?

Besvarelsen tager udgangspunkt i en vurdering af de cyberværnepligtiges kompetencer og profil fra aftagernes perspektiv, som vist i figur 6.2, og inddrager hertil pointer fra analysens del 1, afsnit 5.2 *(Aftagerorganisationer)*. Besvarelsen opsummeres i en delkonklusion.



Figur 6.2: Undersøgelsesdesign - Vurdering af cyberværnepligtige fra et aftagerperspektiv

6.1.1 Kompetencer

De cyberværnepligtige besidder ifølge aftagerne i afsnit 5.2.1 *(Vurdering af cyberværnepligten)*, en god, grundlæggende forståelse for det tekniske domæne, og præsterer på et højt teknisk niveau i forhold til deres uddannelseslængde. I den videnskabelige litteratur optræder et teknologi-fokuseret perspektiv. Her fremlægges teknologi og teknologisk best practice som afgørende fundament for opbygning af cyberresiliens i organisationer [35, 11, 25, 21, 9]. Det er gennemgående i litteraturen, at det tekniske personale har en afgørende rolle for cyberresiliens i organisationer (Se bilag [K1], s. 9). Der er behov for mange forskellige kompetencer, men det er primært de tekniske kompetencer, som efterspørges. Dette er en mangelvare på nationalt plan jf. afsnit 5.3.1 *(National Cyberindsats)*. Der er konsensus om, at tekniske kompetencer spiller en afgørende rolle, og er forudsætningsskabende for cybersikkerhed.

De cyberværnepligtiges grundlæggende forståelse for det tekniske domæne, samt deres attitude og vilje til at udvikle sig, medfører, at mange bestrider junior-stillinger direkte efter uddannelsen. Dette sker på trods af deres relativt korte uddannelsestid. Juniorstillingerne er oftest SOC-relaterede. Betydningen af netop SOC-center og SOC-funktionen adresseres også i litteraturen, og fremhæves som et vigtigt element i at skabe cyberresiliens i organisationer. Dog kan en SOC-løsning være omkostningstung især for mindre virksomheder

[21]. Det kan især være problematisk for mindre virksomheder, da truslen mod dem kan være signifikant og at CFCS som myndighed ikke direkte har som opgave at henvende sig til disse, jf. afsnit 5.3.1.

I forlængelse af førnævnte SOC-funktion, fremgår det desuden, at cyberværnepligtige bestrider funktioner, der har til direkte formål at udfylde "detect- & response-funktioner. Disse udspringer af en frameworkbaseret tilgang til cyberresiliens, der er fremherskende i litteraturen [7, 38, 5, 19, 10, 21, 18, 13]. Cyberværnepligtiges funktioner relateret til frameworks, anvender deres tekniske kompetencer til at bidrage til opbygning af organisatorisk resiliens indenfor visse dele af frameworks.

Netop de tekniske kompetencer, som de cyberværnepligtige besidder, kan derfor være med til at imødekomme de stigende cybertrusler mod Danmark. De cyberværnepligtiges tekniske kompetencer passer ifølge aftagerne godt ind i deres organisationer. De tekniske kompetencer vurderes hermed relevante og tidssvarende, i forhold til de stillinger de bestrider.
I forlængelse af de tekniske kompetencer, fremgår også organisatoriske kompetencer. Aftagerne vurderer i afsnit 5.2.1 de cyberværnepligtiges organisatoriske kompetencer som gode, hvor kommunikation og organisationsforståelse særligt fremstår. Organisatorisk forståelse og effektive kommunikationsveje fremhæves i litteraturen som medskabende til øget cyberresiliens i organisationer [12, 24]. De cyberværnepligtiges vurderede evne til at kommunikere og samarbejde, er udgangspunktet for godt teamwork, hvilket også fremhæves som vigtigt. Dette og vidensdeling giver bedre mulighed for, at respondere på hændelser ift. cyberresiliens [12, 24]. Ligeledes italesætter aftagerne, hvordan cyberværnepligtiges organisationsforståelse gavner især større organisationer. Sammenholdes organisationsforståelsen med litteraturen fremkommer et bedre afsæt i at forstå deres omkringliggende miljø og kontekst [2].

Aftagerne vurderer de cyberværnepligtiges manglende ledelsesmæssige kompetencer som irrelevante ift. den funktion som de ofte bestrider i aftagerorganisationerne. Pointen er gennemgående, da de cyberværnepligtige sjældent indtager en ledende rolle. Litteraturen beskriver et lignende medarbejderperspektiv, der ikke er ledelsesdrevet. Her påpeges især vigtigheden af kollektivt ansvar fordelt på alle organisationslag [24, 22, 38, 16, 11]. Dertil er en intern rollefordeling og vidensdeling vigtig, da det styrker evnen til at respondere [16, 11, 27]. I dette perspektiv fokuseres der på medarbejderen som central for at opbygge cyberresiliens.

6.1.2 Profil

For de cyberværnepligtiges profil, fremhæver aftagerne særligt omstillingsparathed, nysgerrighed for cybersikkerhed og evnen til at tilegne sig ny viden. Lignende profiltræk fremtræder i litteraturen, og er særligt relevante for opbygning af cyberresiliens, hvilket ses i temaerne *Awareness og Kultur* og *Organisatorisk Læring* (bilag [K1], s. 13-15). Her er begreberne træning, adaption og omstillingsparathed omdrejningspunkt for førnævnte afsnit. Det beskrives, hvordan sikkerhedskultur opbygges i en organisation gennem træning og uddannelse af personale i en top-down tilgang, men også at opbygning af sikkerhedskultur kræver, at ledelsen formår at lære af personalet igennem bottom-up tilgange [36, 20, 39, 28, 3, 25, 37]. De cyberværnepligtiges evne til at tilegne sig ny viden er derfor første led i, at skabe en god sikkerhedskultur. Netop sikkerhedskulturen er et vigtigt skridt mod opbyggelse af cyberresiliens. Den fulde effekt af veluddannet personale opnås først, når ledelse og medarbejdere formår at lære gensidigt af hinanden. De cyberværnepligtiges motivation for cyberdomænet og lærenemhed italesættes som særligt vigtigt, og dette profiltræk fremstår vigtigere end et specifikt sæt af kompetencer. Dette kan forklares med, at profil ikke kan tillæres på samme måde som kompetencer. De cyberværnepligtiges profil kan dermed være med til at skabe forudsætning for en bedre sikkerhedskultur.

6.1.3 Delkonklusion - vurdering af cyberværnepligt

De cyberværnepligtige besidder en god, grundlæggende forståelse for det tekniske domæne, og varetager typisk specifikke tekniske opgaver. De cyberværnepligtiges funktion er typisk indlejret som en del af en større sikkerhedsstruktur, der anvender en framework-baseret tilgang. Her er deres organisatoriske forståelse samt evne til at kommunikere og samarbejde fordelagtig. De cyberværnepligtige besidder ifølge aftagerne ikke væsentlige ledelsesmæssige kompetencer, hvilket dog ikke vurderes som problematisk i deres typiske jobfunktion. Særligt fremtrædende for de cyberværnepligtige er deres nysgerrige og motiverede personprofil, hvilket medfører, at de nemt kan anvendes i forskellige funktioner.

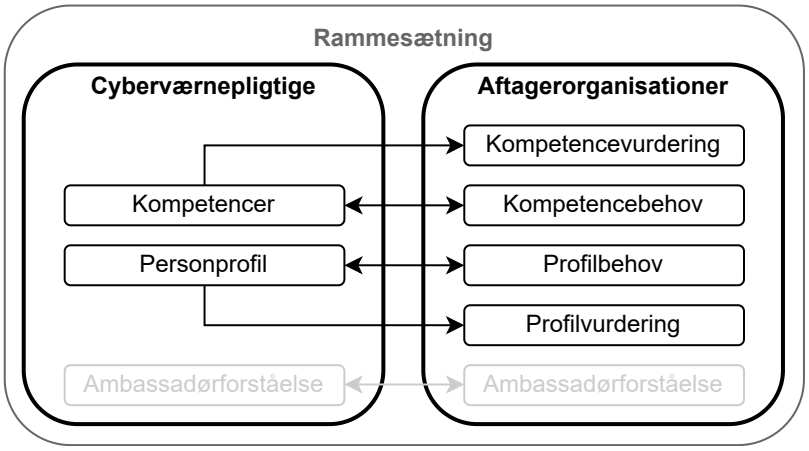
6.2 Forhold mellem cyberværnepligtige og aftagerorganisationer

Dette afsnit har til formål at besvare underspørgsmål 2, som lyder:

> *Hvordan er forholdet mellem cyberværnepligtiges kompetencer og profil, og aftagerorganisationernes kompetence- og profilbehov?*

Besvarelsen tager udgangspunkt i undersøgelsesdesignet vist i figur 6.3. Underspørgsmålet besvares ved at analysere de cyberværnepligtiges kompetencer og profil gennem: analyse og selvevaluering, afsnit 5.1 *(Cyberværnepligtige)*; samt aftagernes vurdering af disse fra underspørgsmål 1, afsnit 6.1 *(Vurdering af Cyberværnepligtige)*. Dette sættes overfor aftageres kompetence- og profilbehov, der afdækkes gennem de cyberværnepligtiges nærmeste ledelse i aftagerorganisationer jf. afsnit 5.2.3 *(Behov hos aftagerorganisationer)*.

Slutteligt sammenholdes cyberværnepligtiges kompetencer og profil med behovet for disse ved aftagerorganisationerne. Besvarelsen opsummeres i delkonklusionen. Afsnittet er struktureret ved først at undersøge hhv. tekniske-, organisatoriske- og ledelsesmæssige kompetencer. Herefter følger undersøgelse af profil, og afsluttes med at sammenholde disse.



Figur 6.3: Undersøgelsesdesign - Kompetence- og profilforhold

6.2.1 Kompetenceforhold

Tekniske kompetencer

Af konkrete tekniske kompetencer nævner aftagerne i afsnit 5.2.3 hyppigst netværksforståelse som nødvendig og forudsætningsskabende kompetence for at opbygge cybersikkerhed, hvilket er identisk med de cyberværnepligtiges primære selvvurderede tekniske kompetence. Ydermere er cyberværnepligtiges fokus på threat-hunting og red/blue teaming sammenfaldende med aftagerorganisationernes behov for sikkerhedsanalyse- og vurdering, samt sikkerhedshændelseshåndtering. Hos begge interessentgrupper fremhæves en generel forståelse for det tekniske domæne som afgørende. I forholdet mellem de cyberværnepligtiges kompetenceprofil og aftagerorganisationernes kompetencebehov, er der en høj grad af overensstemmelse. Litteraturen påviser, at tekniske kompetencer og forståelse er forudsætningsskabende for, at medarbejdere kan bidrage til cyberresiliens i organisationer [24, 22, 38, 16, 11]. Derudover bidrager dette til en operationalisering af frameworks, hvor tekniske kompetencer anvendes primært i form af netværksforståelse og sikkerhedsanalyse, hvilket typisk indgår i *protect-* og *detect-* faserne. De tekniske kompetencer afspejler de cyberværnepligtiges typiske funktion i en organisation, hvor deres bidrag ofte indgår som en del af et større cybersikkerhedsframework jf. afsnit 6.1. Yderligere understøttes dette af aftagerne, der påpeger at de cyberværnepligtige typisk indgår som en del af en større organisatorisk helhed. Det vurderes derfor, at der er en høj grad af overensstemmelse mellem de cyberværnepligtiges tekniske kompetencer og aftagernes vurdering samt behov for disse.

Organisatoriske kompetencer

I delkonklusionen til underspørgsmål 1 fra afsnit 6.1.3 konkluderes det, at de cyberværnepligtige besidder en organisationsforståelse. Dette gør dem let anvendelige i funktioner i en typisk stor organisation, som har en framework-baseret tilgang til cyberesiliens. Det er i overensstemmelse med de cyberværnepligtiges selvvurderede kompetencer, hvor samarbejde, struktur og kommunikation beskrives som de primære organisatoriske kompetencer. Disse er alle kompetencer, som egner de cyberværnepligtige til at indgå i en større organisatorisk enhed. De større organisationer anvender ofte en standardiseret og framework-baseret tilgang til cyberresiliens [7, 38, 5, 19, 10, 21, 18, 13], hvor de omtalte kompetencer i høj grad ses anvendelige. Tilgangen er dog ressourcekrævende og kan udfordre især SMV'er [25], hvilket gør de cyberværnepligtige mindre relevante i denne type virksomheder. Det vurderes derfor, at de cyberværnepligtige er bedst egnet til større virksomheder, men begrænset egnet til mindre virksomheder.

Aftagerorganisationerne nævner yderligere behov for organisatoriske kompetencer i afsnit 5.2.3, hvor særligt risikostyring og framework-forståelse fremhæves. Både risikostyring [32, 36, 19, 27, 10] og frameworks [7, 38, 5, 19, 10, 21, 18, 13] har et stort fokus i litteraturen for at opbygge cyberresiliens, men nævnes i lav grad af de cyberværnepligtige, og er ikke en del af deres organisatoriske kompetencer. Der ses derfor en lagdeling i de cyberværnepligtiges organisatoriske kompetencer, hvor de cyberværnepligtige besidder samarbejdsmæssige og kommunikative kompetencer til at indgå i teams og større enheder, men mangler organisatoriske værktøjer til at lede resilienstiltag som f.eks. frameworks eller risikostyring. De organisatoriske kompetencer er mest relevante på manuelt eller udførende niveau, fremfor i en planlægnings- eller ledelsesfunktion. Denne uoverensstemmelse konkretiseres f.eks. gennem, at der i Forsvaret er brug for en cyberuddannelse på konstabel-, befalingsmands- og officersniveau jf. 5.2 *(Aftagerorganisationer)*. Ligeledes nævnes det, at der er behov for et bredt spektre af cyberprofiler jf. afsnit 5.2.3 og 5.3.1 *(National Cyberindsats)* til at imødegå det nu brede spektre af cybertrusler jf. 5.3.1.

Ledelsesmæssige kompetencer:

Som et overordnet behov hos aftagerorganisationerne, spiller ledelsesmæssige kompetencer en salient rolle i opbygningen af cyberresiliens jf. afsnit 5.2.3. Samlet set er der i litteraturen fokus på, at ledelse er vigtigt og nødvendigt for en effektiv og prioriteret cyberindsats [22, 28, 9, 37], og der er konsensus om, at ledelse spiller en vigtig rolle i forbindelse hermed. Med afsæt i data fra aftagerne, fremhæves en række kompetencer, der også i udpræget grad fremstår i den videnskabelige litteratur: særligt GRC-kompetencer (Governance: [38, 28, 37, 13, 20, 28], Risk management: [32, 36, 20, 19, 36, 19, 10] og Compliance: [39]). Derudover fremhæver aftagerne desuden strategi [20,10], kriseledelse [16, 11, 27] og stakeholder-kommunikation [12, 22, 20, 3, 35], som efterspurgte ledelsesmæssige kompetencer. Governance nævnes af de cyberværnepligtige, som en af de mest fremtrædende konkrete ledelsesmæssige kompetencer de besidder, jf. afsnit 5.1.1 *(Kompetencer)*. Under observationsstudiet formåede de cyberværnepligtige dog kun i lav grad at styre en fælles indsats og tage

effektive beslutninger under pres. Det var ligeledes problematisk at koordinere og kommunikere en fælles strategi jf. afsnit 5.1.1. I forlængelse heraf udtrykker flertallet af de nuværende cyberværnepligtige selv en manglende indsigt overfor deres egne ledelsesmæssige kompetencer (66,7%). Selvom de cyberværnepligtige ikke besidder nævneværdige ledelsesmæssige kompetencer, inddrages pointen fra underspørgsmål 1: at de cyberværnepligtige ikke har ledelsesmæssige kompetencer, er givet set irrelevant, da de sjældent bestrider en ledelsesmæssig rolle i organisationerne, hvor disse kompetencer er relevante eller afgørende. I forlængelse heraf, forekommer en stigning i vægtningen af de ledelsesmæssige kompetencer fra nuværende til tidligere cyberværnepligtige, hvor tidligere cyberværnepligtige vurderer egne ledelsesmæssige kompetencer højere, jf. figur 5.5. Dette kan være et udtryk for, at erfaring gennem ansættelse giver de cyberværnepligtige større tillid til deres egne ledelsesmæssige kompetencer, hvilket er med til at opkvalificere dem og gøre dem mere relevante. Det vurderes dog, at de cyberværnepligtiges manglende ledelsesmæssige kompetencer kan agere barriere for fremtidige karrieremuligheder. Dette skyldes, at manglende ledelsesmæssige kompetencer kan reducere muligheden for organisatorisk avancering i aftagerorganisationer, og dermed begrænse langsigtede udviklingsmuligheder. Dette understøttes yderligere af mangel på formel faglært eller kvalifikationsgivende uddannelse jf. afsnit 5.2.1*(Vurdering af cyberværnepligten)*.
De cyberværnepligtige udmærker sig især på de tekniske- og organisatoriske kompetencer. De ledelsesmæssige kompetencer fremstår ikke fremtrædende, men dette forhold vurderes mindre betydningsfuldt af aftagerne, grundet de funktioner cyberværnepligtige typisk indtager i større organisationer. Sidstnævnte skal forstås i relation til den indledningsvise ansættelse af cyberværnepligtige.

6.2.2 Profilforhold

Motivation

Cyberværnepligten er i høj grad en motivationsfaktor, for at fortsætte arbejdet med cybersikkerhed for de cyberværnepligtige. Hele 93% svarer enig eller meget enig i, at cyberværnepligten har motiveret dem til at arbejde videre med, eller uddanne sig videre indenfor, feltet jf. afsnit 5.1.2 *(Profil)*. Særligt motivation og interesse for cyberdomænet er ligeledes et fokuspunkt for aftagerne, som ofte prioriterer cyberværnepligtige netop på grund af deres særlige motivation og interesse for feltet. Motivation og interesse anses af aftagere som vigtigere end kompetencer jf. afsnit 5.2.3. Den motiverede personprofil, som cyberværnepligten bidrager til at støbe, er derfor afgørende for vurdering af cyberværnepligtens relevans. At cyberværnepligten opleves som motiverende kan skyldes, at de cyberværnepligtige gennem fællesskab, fælles træning og uddannelse indenfor cybersikkerhed indgår i en fælles sikkerhedskultur jf. afsnit 5.2 *(Aftagerorganisationer)*. Netop fælles træning og uddannelse er i den videnskabelige litteratur også hyppigt forekommende, og er omdrejningspunkt for at danne en sikkerhedskultur og awareness i organisationer (Se bilag [K1], s. 13-14). Ydermere forventes sikkerhedskulturen at blive forstærket af cyberværnepligtens rammer, hvor de cyberværnepligtige indgår i et fællesskab om cybersikkerhed på daglig basis. Netværk, fællesskab og sammenhold er også signifikante

for de cyberværnepligtige, hvor tæt på 100% af de cyberværnepligtige svarer meget enig eller enig til, at cyberværnepligten har bidraget med relevant netværk indenfor cybersikkerhed, samt at cyberværnepligten har bidraget til fællesskabsfølelse og sammenhold jf. afsnit 5.1.2. De særlige forhold cyberværnepligtige uddannes under, hvor de bor og lever, er et unikt træk der er knyttet til deres militære baggrund og ikke forefindes ved andre lignende uddannelser jf. afsnit 5.2. Fællesskabet tydeliggøres af, at mange indgår i et frivilligt netværk efter cyberværnepligten. Udover at netværket stort set er Forsvarets eneste kontaktkanal til de tidligere cyberværnepligtige, bibeholdes motivation og fællesskab iblandt tidligere cyberværnepligtige i dette regi. Det frivillige netværk tillægger derfor cyberværnepligtigen yderligere mening, værdi og relevans. Dette skyldes, at de cyberværnepligtige oplever et udviklende og meningsfyldt fællesskab, hvor omdrejningspunktet er den fælles interesse for cyber. Ydermere holdes de tidligere cyberværnepligtige ajourførte i et omskifteligt domæne jf. afsnit 5.1.2 og 5.2.5 *(Ambassadørrollen)*.

Betydning af militær baggrund

I afsnit 5.1 fremgår det, at de cyberværnepligtige i højere grad finder cybersikkerhed motiverende sammenlignet med arbejdet som soldat. Deres interesse er cybersikkerhed fremfor soldatervirket. Ydermere vurderer aftagerne i afsnit 5.2.1 *(Vurdering af cyberværnepligten)* kun i nogen grad, at de cyberværnepligtiges militære baggrund har betydning. Til trods for, at de cyberværnepligtiges militære baggrund ikke direkte tillægges stor betydning af aftagerne eller de cyberværnepligtige selv, kommer afledte og indirekte effekter alligevel til udtryk. Aftagerne svarer i høj grad "enig"eller "meget enig"til, at de cyberværnepligtige opleves som punktlige (ca. 60%), læringsvillige (ca. 55%) og holdspillere (ca. 70%). Punktlighed, læringsvillighed og holdånd kan være et udtryk på netværk og sammenhold, som de cyberværnepligtige indgår i, hvilket, som beskrevet ovenfor i 5.1.2, tillægges stor værdi af de cyberværnepligtige. Det at arbejde sammen i teams, er netop en pointe som adresseres i 5.3.3, som et kendetegn ved Forsvarets uddannelser. Den militære baggrund hos de cyberværnepligtige har derfor betydning for udviklingen af de cyberværnepligtiges personprofil. Netop læringsvillighed, netværk og motivation vurderes af aftagerne at være udslagsgivende for ansættelse af de cyberværnepligtige jf. 5.2, og den militære baggrund kan derfor tillægges værdi, til trods for kun at komme indirekte til udtryk.

6.2.3 Delkonklusion - forholdet mellem cyberværnepligt & aftagerorganisation

Der er en høj grad af overensstemmelse mellem de cyberværnepligtiges tekniske kompetencer og de behov, som aftagerorganisationerne har. Dette skyldes primært de cyberværnepligtiges kompetencer indenfor netværksforståelse og sikkerhedsanalyse. Disse understøtter den organisatoriske cyberresiliens, eftersom de cyberværnepligtige kan indgå som en integreret del af en større cybersikkerhedsorganisation. Det er mest udpræget i organisationer, hvor de cyberværnepligtige fyldestgørende varetager specifikke funktioner i relation til sikkerhedsframework.

I forlængelse heraf, besidder de cyberværnepligtige organisatoriske kompetencer som *samarbejde* og *kommu-*

nikation, og er velegnede i større organisationer med dedikerede cybersikkerhedsenheder, hvor der er stort behov for koordination, vidensdeling og bredere forståelse. Derimod mangler de cyberværnepligtige specifikke organisatoriske kompetencer som risikostyring og frameworkforståelse, som udgør et behov hos aftagerorganisationerne.

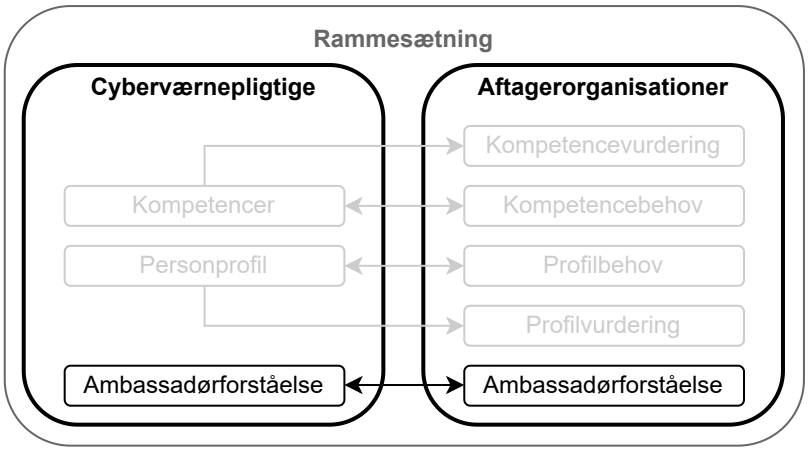
De cyberværnepligtiges ledelsesmæssige kompetencer er begrænsede, og imødekommer ikke aftagerorganisationernes behov for ledelseskompetencer på et generelt plan. Dog fremhæver aftagerne, at manglen på ledelsesmæssige kompetencer hos de cyberværnepligtige er irrelevante, eftersom det typisk ikke falder inden for deres arbejdsområde. Der observeres en ændring i vurdering af egne kompetencer fra kategorien nuværende til tidligere cyberværnepligtige, der indikerer at de opnår højere selvindsigt efter endt uddannelse. Karakteriserende for de cyberværnepligtiges profil, fremhæves særligt *motivation* og *interesse for feltet*, hvilket imødekommer aftagernes profilbehov. Til trods for, at den militære baggrund ikke har direkte betydning hos aftagere eller cyberværnepligtige, får den militære baggrund indirekte betydning ved at bidrage til *samarbejde, punktlighed* og *læringsvillighed*.

6.3 Ambassadørforståelse

Dette afsnit har til formål at besvare underspørgsmål 3, som lyder:

> *Hvordan manifesteres rollen som ambassadør for god IT-sikkerhed i praksis?*

Afsnittet undersøger, hvordan rollen som ambassadør for god IT-sikkerhed manifesteres i praksis ved henholdvis cyberværnepligtige og aftagere, som vist i figur 6.4. Besvarelsen tager udgangspunkt i afsnit 5.2.5 *(Ambassadørrollen)* og 5.1.3 *(Ambassadørforståelse)* og opsummeres i delkonklusion 6.3.2.



Figur 6.4: Undersøgelsesdesign - Ambassadørforståelse

6.3.1 Ambassadørrollen

Ambassadørrollen bliver italesat som værende en vigtig og prioriteret del af Forsvarets Cyberværnepligt, og aftagerne har generelt et positivt syn på ambassadørrollen, som fremlagt i afsnit 5.2.5. Der bliver i Forsvaret lagt vægt på, at måden de bliver undervist og uddannet på, giver dem et afsæt til at agere ambassadører. Uddannelsen i Forsvaret giver noget særligt i forhold til team og samarbejde, jf. afsnit 5.3.3 *(Cyberværnepligten)*. I den videnskabelige litteratur fremtræder to hovedretninger for ambassadørbegrebet. Den ene retning er knyttet til medarbejderne, og har et bottom-up perspektiv, der kan relateres til Forsvarets forståelse af ambassadørrollen, og hvordan denne manifesteres. Her er cyberresiliens et kollektivt ansvar på tværs af alle organisationslag [24, 22, 38, 16, 11]. I forlængelse heraf ses uddannelse og træning som værende afgørende for, at medarbejdere kan identificere trusler og agere "ambassadør"på team-niveau [22, 36]. Perspektivet på ambassadørrollen foregår på teamniveau, hvilket også afspejler det niveau cyberværnepligtige uddannes på. Litteraturens udlægning af ambassadørbegrebet på team-niveau kan relateres til Forsvarets syn på en ambassadør. Her er ambassadøren en brobygger mellem den tekniske og ikke-tekniske verden, og skaber årvågenhed om cyber i organisationen.

Dette står i kontrast til litteraturens anden retning, hvor et top-down perspektiv er styrende. Her drives sikkerhedskulturen af, at ledelsen agerer champions eller af særligt udvalgte [19]. Ledelsen bliver udslagsgivende for etableringen af en sikkerhedskultur. I dette perspektiv skal ledelsen tage ansvar fremfor medarbejderne, hvilket afspejles i aftagernes syn på manifestationen af de cyberværnepligtige, som ambassadører i aftagerorganisationer. I afsnit 5.2.5, er der konsensus om, at aftagerne ikke oplever de cyberværnepligtige som ambassadører. Der lægges vægt på, at det ikke giver mening på baggrund af deres uddannelseslængde, samt de stillinger, som de typisk bestrider. Ambassadørrollen har ikke været udslagsgivende for ansættelsen af cyberværnepligtige, hvilket vurderes at være knyttet til den rolle de skal bestride.

I afsnit 5.1.3 beskrives, hvordan de cyberværnepligtige forstår ambassadørrollen, som en person der videreformidler, er budbringer eller lærer andre om god cybersikkerhed. Sekundært som en person, der er engageret, hvilket stemmer overens med aftagernes generelle forståelse for rollen. De cyberværnepligtige ser deres rolle som ambassadør mere prominent i samfundet frem for Forsvaret. Mellem tidligere og nuværende cyberværnepligtige, ses en bevægelse fra ambassadør som "engageret"til en "videreformidler"eller "budbringer". I takt med at de opnår praksis erfaring, ændres opfattelse af rollen som ambassadør som vist i figur 5.8 og 5.9, hvilket læner sig op ad litteraturens bottom-up perspektiv på 'ambassadørrollen' [22, 36].

Hos de cyberværnepligtige findes en forståelse af, at de skal agere ambassadører jf. figur 5.9, hvilket er i overensstemmelse med den rammesættende forståelse fra afsnit 5.3.3. Der fremgår et fælles syn på rollen, der dog er i modsætningsforhold til den opfattede manifestering i praksis, som ses ved aftagerorganisationerne jf. afsnit 5.2.5. Denne diskrepans mellem interessentgrupper er udpræget og interessant i form af, om de cyberværnepligtige kan forventes at agere ambassadører i deres stillinger. Diskrepansen kan også skyldes ambassadørbegrebets semantik, hvor Forsvarets formulering af ambassadørbegrebet konstrueres med en anden betydning end hvad aftagerorganisationerne fortolker den som. Yderligere kan dette nuanceres af cyberværnepligtens uddannelseslængde på 6 måneder, kontra den litterære beskrivelse af 'ambassadørrollen' (Bilag K1, s. 9 [22, 36] og s. 14 [19]), hvilket afspejler en mangefacetteret rolle. Fra aftagerorganisationerne ses desuden, at det ikke entydigt forventes, at de kan agere ambassadører i deres funktioner og med deres uddannelsesniveau jf. afsnit 5.2.5.

6.3.2 Delkonklusion

Der hersker i litteraturen, ved aftagere og cyberværnepligtige konsensus om, at ambassadørrollen indenfor cybersikkerhed er et positivt begreb. Der er dog ikke enstemmighed ift. hvorvidt de cyberværnepligtige indtager denne, og dermed agerer ambassadører i aftagerorganisationerne i praksis, yderligere om de cyberværnepligtige overhovedet er egnede til at indtage rollen, set fra et aftagerperspektiv. Det vurderes, at ambassadørrollen er en ønskværdig rolle, som har svært ved at manifestere sig ved de cyberværnepligtige i deres hverdag. De cyberværnepligtiges selvbillede som ambassadører afspejles i Forsvarets egen organisation, men ikke i praksis ved aftagerorganisationerne. Det skyldes tildels, at ambassadørbegrebet optræder tvefoldigt, hvor Forsvaret ser begrebet på team-niveau og aftagerne typisk relaterer det til ledelsesniveauet. Førstnævnte kan i nogen grad praktiseres, men kun hvis de cyberværnepligtige befinder sig organisatorisk, hvor de har mulighed for at agere herefter. Ambassadørbegrebet i et ledelsesperspektiv ses ikke udfoldet hos de cyberværnepligtige. Uddannelsen i sin nuværende form skaber ikke forudsætning for at kunne indtage og opfylde denne betydningsfulde rolle, og derfor opfattes de cyberværnepligtige i aftagerorganisationerne ikke som ambassadører.

6.4 Opsummering af analyse del 2

Det kan for analysens del 2 opsummeres, at der er gennemgående fund indenfor aftagernes vurdering af profil, kompetencer og ambassadørrollen, der reflekteres i det teoretiske perspektiv. Aftagerne vurderer de cyberværnepligtige til at have god forståelse for det tekniske- og organisatoriske domæne. Derimod vurderes de ikke at have nævneværdige ledelsesmæssige kompetencer. Dette opfattes ikke problematisk, da de cyberværnepligtige sjældent bestrider ledelsesmæssige roller. Derudover er deres nysgerrige og læringsvillige profil afgørende for deres relevans i større organisationer. Der er høj grad af overlap mellem aftagerorganisationernes tekniske og organisatoriske behov og de kompetencer, som de cyberværnepligtige bidrager med. De cyberværnepligtige forstår deres tekniske domæne og organisationsstruktur. De kommer med en profil, som er læringsvillig, motiveret og har forståelse for cyber. Sammensluttes aftagernes vurdering og behov med den faktiske udlægning af de cyberværnepligtiges kompetencer og profil, giver det et holistisk billede af en medarbejder, som er relevant for opbygning af cyberresiliens. Dette skyldes at deres kompetencer er gode, men ikke fastgroede og derfor er omstillingsparate. De besidder en forståelse for organisationen og med en sammensmeltning af deres kompetencer og profil, bliver grundlaget for cyberresiliens muliggjort. De cyberværnepligtige er ansat i stillinger, hvor berøringsfladerne er cyberrelateret, og med den rette ledelse, er deres profiler relevante kandidater til, at skabe cyberresiliens. Dette kommer til udtryk igennem litteraturens linse på cyberresiliens og aftagernes egne udlægninger af forholdet mellem kompetence- og profilbehov.
De cyberværnepligtiges rolle som ambassadør, bliver i analysen påvist ikke at manifestere sig sammenligneligt med kontekst og den overbevisning, som Forsvaret har sat rollen i verden med. Ambassadørrollen stikker ud fra det samlede billede, som er blevet tegnet af de cyberværnepligtige i analysen. Det vurderes, at rolle ikke manifesterer sig i praksis, og at der er en tvetydig opfattelse af rollen mellem Forsvaret og aftagerorganisationerne. Litteraturen påviser, at en ambassadør er relevant for opbyggelsen af cyberresiliens, men set i det store billede og med afsæt i aftagernes behov og vurdering, er rollen ikke afgørende i netop optegningen af de cyberværnepligtiges billede i praksis.

Kapitel 7

Diskussion

Afsnittet har til formål at diskutere centrale fund fra analysen, der kan føre til konkrete anbefalinger til anvendelse i praksis. Anbefalingerne er forankret i analysens fund, og tager ikke afsæt i politisk, militær eller økonomisk prioritering. Diskussionen bidrager, i kombination med de teoretiske perspektiver og analysens del 1 og 2 samt, til konklusionen, og derved besvarelse af problemformuleringen, som vist i figur 7.1.

Figur 7.1: Diskussionens placering i undersøgelsesstrukturen

7.1 Anvendelse i praksis

Nedenstående afsnit har til hensigt at bidrage med konkrete anbefalinger på baggrund af analyse af Forsvarets cyberværnepligt og diskutere centrale fund. Anbefalingerne er adresseret Forsvarets ressortområde, da det er her uddannelsesansvaret og uddannelsen findes.

7.1.1 Skalering af cyberværnepligt

Fra afsnit 1 *(Indledning)*, 5.2.3 *(Behov hos aftagerorganisationer)* samt 5.3.3 *(Cyberværnepligten)* ses klare indikationer på, at cybertruslen stiger, samt at behovet for cyberkompetencer øges hos aftagere og på nationalt plan. Samtidigt erkendes det fra ministerielt niveau, at det årlige volumen på 32 cyberværnepligtige langt fra

dækker nuværende behov. Det er derfor relevant at diskutere muligheden for at skalere cyberværnepligten og øge volumen. Der er bred og klar konsensus fra aftagere om, at behovet er stort jf. 5.2.3 og at de efterspørger de kompetencer som cyberværnepligtige besidder. Samtidigt er markedet umættet, og styrkeproduktionen på 32/år vurderes som væsentligt under behov. Fra rammesættende interessenter fremgår det jf. 5.3.3 desuden, at målrammen for cyberværnepligtige er opfyldt, uanset om de cyberværnepligtige tager arbejde offentligt eller privat. Mere end 93% af de cyberværnepligtige arbejder fortsat indenfor domænet jf. 5.1.2 *(Profil)*, og hele 95% anser cyberværnepligtsuddannelsen som grundlag herfor. Det er meningsfyldt at overveje, hvorledes uddannelsen kan opskaleres i en konstellation, hvor særligt indholdet bibeholdes relevant og opdateret, kompetenceprofilen fastholdes og person-profilen bevares stærk og attraktiv gennem selektering og teamwork. Det vurderes vigtigt, at kvaliteten af cyberværnepligten bibeholdes, og denne ikke kompromitteres af kvantitet jf. 5.2.3. Uddannelsen bidrager med en stærk og unik profil i et efterspurgt marked. Skalering bør ske indenfor samme rammer, og med samme uddannelsesprofil.

Anbefaling: Det anbefales at skalere Forsvarets Cyberværnepligt med afsæt i et behovsestimat i Forsvarets egen organisation, samt ved større virksomheder, primært indenfor kritisk infrastruktur. Behovsestimat bør ligge til grund for eksakt antal. Det anbefales i forbindelse hermed, at afdække konkrete karriereveje og ansættelsesmuligheder internt i Forsvaret for at kunne anvende de cyberværnepligtige mest relevant.

7.1.2 Cyberuddannelse på flere niveauer

Som det fremgår i afsnit 5.3.3 *(Behov hos aftagerorganisationer)*, er der for cyberværnepligtige en fastholdelsesgrad på 40 % i Forsvaret. Dette tal er højt sammenlignet med almindelige værnepligtige. Dog identificeres betragtelige fastholdelsesproblematikker, der primært er knyttet til ansættelse i Hæren. Dette er til trods for, at Forsvaret, og særligt Hæren, står overfor en massiv rekrutteringsopgave jf. 5.3.3. De cyberværnepligtige er uddannet på et grundlæggende niveau, og indtager i Forsvaret primært stillinger på konstabelniveau (manuelt niveau) jf. 5.2.1 *(Vurdering af cyberværnepligten)*. Der eksisterer ikke formelle karriereveje eller karriereretninger indenfor cyber i Forsvarets organisation, og derved forudses et kompetencespild i overgangen fra manuelt niveau til ledelsesstillinger. Integrationen af cyber kan med fordel anvendes på tværs af niveauer og domæner i militære operationer, men er samtidigt udfordret af en ressourcemæssig udfordring på personelsiden jf. 5.3.1 *(National Cyberindsats)*.

Anbefaling: Det anbefales at afdække, hvordan man med fordel kan fastholde en større personelmængde og oprette uddannelser i Forsvaret til befalingmands- og officersniveau. Disse bør være specifikke og målrettede cyberuddannelser. Dette initiativ vil bidrage med konkrete og kompetente cyberkompetencer på tværs af uddannelsesniveauer og værn. Dette kan samtidig optimere brugen af cyberkompetencer på tværs af domæner. Slutteligt vil en længere karriere i Forsvaret indenfor cyber afhjælpe rekrutteringsudfordringen og potentielt reducere fastholdelsesproblematikken i domænet, men det kræver en form for meningsfuld karrierevej. Det

anbefales at oprette målrettede cyberuddannelser på tværs af niveauer. Disse skal have højere taksonomisk niveau, og ikke blot være kortere suppleringskurser til de eksisterende uddannelser. Dette skal bidrage med kompetencer, der kan operationaliseres i operativ handling.

7.1.3 Udkast til cyberkonstabeluddannelse

Det mest oplagte videreuddannelsesniveau efter cyberværnepligt er konstabeluddannelse. I mangel på en formel cyberkonstabel, kan Forsvaret gøre brug af nedenstående konkrete forslag som anbefaling til uddannelsesdesign. Som beskrevet i 5.2.1 *(Vurdering af cyberværnepligten)* besidder cyberværnepligtige qua deres baggrund typisk faglærte stillinger med en ufaglært baggrund. Dette kan fastholde cyberværnepligtige på et uhensigtsmæssigt uddannelsesniveau over længere tid ift. deres kompetencer. Det anbefales derfor, at strukturere uddannelse, der efter en given tid gør dem til faglærte og dermed virker kvalifikationsgivende. Cyberkonstabeluddannelse ses som en oplagt første karrierevej for Forsvarets Cyberværnepligtige efter endt værnepligtuddannelse.

I forbindelse med den nuværende uddannelse, identificeres et behov for praksiserfaring og driftskompetencer jf. 5.2.1. Disse mangler, samt erfaring med specifikke områder, kan med fordel foregå i form af praktikophold/elev-plads i samme konfiguration, som ellers findes på uddannelser med *kvalifikationsramme for livslang læring, niveau 4*. Praktikophold kan placeres internt i Forsvarets organisation, eller i virksomheder tilhørende kritisk infrastruktur, der typisk er af en størrelse og prioritet, som kan håndtere en større personalemængde. Ved førstnævnte, vil det være muligt at sprede uddannelsesophold over flere værn, for herigennem at gøre cyberkonstabler mere bredt anvendelige i Forsvarets organisation, hvilket kan bidrage til at øge anvendelsesmulighederne for disse. Formaliseret faglært uddannelse, vil bidrage positivt til kompetence- og kvalifikationsprofilen for personellet, og det kan være med til at øge fastholdelsen. Dette vil være attraktivt for både medarbejderen og Forsvaret som organisation. Denne pointe kan dog diskuteres, da flere aftagerorganisationer efterspørger specifikke kompetencer jf. 5.2 *(Aftagerorganisationer)*, men vægter profil fremfor kompetence jf. 5.2.3 *(Behov hos aftagerorganisationer)*.

Anbefaling: Det anbefales at oprette en faglært cyberkonstabeluddannelse til niveau 4 i kvalifikationsramme for livslang læring. Uddannelsen skal være baseret på videreuddannelse, hvor særligt elev-ophold i driftsorganisationer indlægges. Disse bør placeres bredt i Forsvarets organisation, og evt. suppleres med ophold i virksomheder tilhørende kritisk infrastruktur. Uddannelsen skal medføre et kvalifikationsgivende uddannelsesbevis, der kan anvendes ifm. akkreditering til andre uddannelser på højere niveau.

7.1.4 Drop ambassadørbegrebet

Som diskuteret og analyseret i afsnit 6.3.1 *(Ambassadørrollen)*, manifesteres rollen som ambassadører kun i mindre grad i praksis, da de cyberværnepligtige ikke er klædt på eller uddannet til at kunne indtage denne meningsfuldt. Aftagernes forståelse af begrebet er forankret i et ledelsesperspektiv. Internt i Forsvaret italesættes ambassadørrollen positivt med afsæt i en team-baseret forståelse, hvilket kan føre til asymmetri mellem holdning og handling fra Forsvaret til aftagerorganisationer. Dette forstærkes af, at aftagerorganisationerne hverken bemærker rollen i praksis, eller tillægger den synderlig betydning jf. 5.2.5 *(Ambassadørrollen)*. Det kan betyde, at de cyberværnepligtiges narrativ er i dårlig overensstemmelse med den forventning, der er til dem, og den funktion de udfører. Internt i Forsvaret italesættes og dyrkes dermed en rolle, der reelt ikke efterspørges eller bemærkes af aftagerorganisationerne. Dette fokus kunne med fordel flyttes til områder, hvor der både er efterspørgsel, og hvor de cyberværnepligtige rent faktisk udmærker sig. Dette argument forstærkes yderligere af, at de cyberværnepligtige selv har svært ved at præcisere hvad begrebet/rollen dækker over jf. 6.3.1, og bruger meget generelle termer til at beskrive det.

Anbefaling: Det anbefales at fjerne fokus fra ambassadørbegrebet og rollen for bedre at bevare de cyberværnepligtiges integritet, samt at have en mere troværdig argumentation internt i Forsvaret ift. hvad de cyberværnepligtige bidrager med. Der er ingen indikation på, at rollen efterspørges eller udfyldes i nævneværdig grad, og derfor bør kommunikationen både internt og eksternt afspejle dette.

7.2 Cyberværnepligtiges bidrag til resiliens

I dette afsnit diskuteres, hvordan de cyberværnepligtige bidrager til at øge den nationale sikkerhed, samt hvorvidt deres rolle retter sig mod cybersikkerheds- eller cyberresiliensperspektivet. Hertil genkaldes definitionerne på cybersikkerhed og cyberresiliens fra afsnit 2.2 *(Metode - teoretisk perspektiv)*. Som beskrevet i afsnit 5.3.1 *(National Cyberindsats)*, ønskes det at højne Danmarks modstandsdygtighed overfor cybertrusler gennem samarbejde, regulativer og kapaciteter på tværs af organisationer og landegrænser, således viden og erfaring akkumuleres. Denne tilgang til opbyggelse af modstandsdygtighed stemmer overens med den videnskabelige litteraturs definition af cyberresiliens, hvor også kommunikation og samarbejde gennem regulativer og frameworks er omdrejningspunkt.

Jf. afsnit 6.2 *(Forhold mellem cyberværnepligtige og aftagerorganisationer)* indgår de cyberværnepligtige typisk i en integreret del af en større cybersikkerhedsstruktur, og de cyberværnepligtiges bidrag til den nationale sikkerhed bør derfor betragtes ligedes. At de cyberværnepligtiges bidrag til en organisation ikke kan betragtes som enkeltstående, er netop hvad retter indsatsen mod resiliensperspektivet frem for sikkerhedsperspektivet til trods for, at de cyberværnepligtiges tekniske kompetenceprofil i høj grad retter sig mod beskyttelse og dermed sikkerhedsperspektivet. De cyberværnepligtiges bidrag til at skabe cyberresiliens, er derfor afhængig af

den organisatoriske kontekst som de indlejres i. Hvis de cyberværnepligtiges rolle efter endt cyberværnepligt f.eks. primært var at implementere firewalls eller lignende, som den eneste sikkerhedsindsats i en organisation, er dette ikke tilfældet. Det skyldes, at cyberresiliens skal betragtes som summen af en række indsatser, der bidrager til en organisations modstandsdygtighed, og derved ikke udelukkende kan være teknisk. At de cyberværnepligtige bidrager til cyberresiliens gennem en større organisatorisk indsats, forstærkes yderligere af de cyberværnepligtiges frivillige netværk, hvor viden også deles på tværs af organisationer. Ydermere bidrager netværket til at sammenholde en teknisk sikkerhedskapacitet, hvilket har interesse i erhvervslivet, hvor tekniske profiler søges. For at de cyberværnepligtige kan bidrage mest effektivt til resiliensskabelsen i en organisation, er dette betinget af, at de cyberværnepligtige placeres i organisationen der komplimenterer deres kompetencer og profil. De organisatoriske rammer har betydning for, i hvilken grad de cyberværnepligtige kan bidrage til cyberresiliensen effektivt. Samtidigt medfører dette, at organisationerne bør have godt kendskab til kompetencer og profil, for rent faktisk at være i en position, hvor de cyberværnepligtige kan placeres mest hensigtsmæssigt. Denne vekselvirkning er baseret på gensidig forståelse.

7.3 Teoretisk perspektiv

Det teoretiske perspektiv, der i undersøgelsen anvendes, er afgrænset til artikler med ledelsesfokus på cyberresiliens, som beskrevet i afsnit 2 *(Teoretisk perspektiv)*. Perspektivet sætter retning for undersøgelsens design jf. 1.3 *(Undersøgelsesdesign)* og metodisk udførsel jf. kap. 3 *(Metode)*. Ledelsesperspektivet anvendes i undersøgelsen, eftersom det ønskes at undersøge, hvordan cyberværnepligten opleves som værende relevant for at højne IT-sikkerheden i aftagerorganisationer. Aftagerorganisationerne repræsenteres af en sikkerhedsansvarlig fra ledelseslaget, og disse har et ledelsesfokus på, hvordan cyberresiliens opbygges i en organisation. Perspektiver fra aftagerorganisationernes ledelsesrepræsentanter og den videnskabelige litteratur kan derfor sammenholdes. Det teoretiske perspektiv bør ikke betragtes som en facitliste for, hvordan cyberresiliens opbygges i en organisation, da den videnskabelige litteratur indeholder paradokser, modsigelser og modsatrettede argumenter for cyberresiliens. Det teoretiske perspektiv, udfolder som navnet indikerer, netop perspektiver på cyberresiliens, fremfor én komplet sammenhængende teori. Derved understreger det teoretiske perspektiv den mangefacetteret virkelighed, som cyberresiliens indbefatter, hvilket øger den teoretiske linses anvendelighed. Perspektivet afspejler derved aftagerorganisationernes virkelighed og kontekst, der forstås som kompleks og med konkurrerende argumenter. Det teoretiske perspektiv egner sig derfor til at fortolke og forstå de cyberværnepligtiges kompetencer, profil og ambassadørforståelse, i relation til aftagerorganisationernes cyberresiliens.

7.4 Metodisk selvrefleksion

Metodisk selvrefleksion indgår i afsnit 3.1.1 som kvalitetskriterie, og uddybes derfor herunder. Metodisk selvrefleksion kommer ikke til udtryk i samme eksplicitte form som transparens, men har i stedet manifesteret

sig undervejs i empiriindsamlingsprocessen, og været en del af den daglige diskussion i undersøgelsesarbejdet. Med afsæt i undersøgelsens empiri, er det derfor relevant at diskutere dennes betydning, både for de metodiske forhold, men også for analysens gyldighed.

7.4.1 Empirisk subjektivitet

Som udgangspunkt er undersøgelsens indsamlede empiri præget af stor subjektivitet, hvor interviewpersoner og respondenter er bedt om at tilkendegive deres egne oplevelser og synspunkter for at evaluere relevansen af cyberværnepligten. Fordelen ved subjektiv data, er muligheden for at tilgå et dybere stratum for at forstå de bagvedlæggende mekanismer og strukturer, som bliver tilkendegivet i interessenternes oplevelser baseret ud fra deres egen kontekst. Dette styrkes yderligere ud fra undersøgelsens evalueringsrationale, hvor interaktion med forskellige interessentgrupper, giver et mere detaljeret billede af cyberværnepligtens relevans. Hertil er brugen af flere, både kvantitative og kvalitative datakilder, med til at skabe mere dybde og nuance i interessenternes tilkendegivelser. Derimod kan undersøgelsens sampling-tilgang, kombineret med empiriens subjektive natur, udgøre et kombineret bias i empirigrundlaget, som også er nævnt i afsnit 3.4. Grundet dette er der risiko for, at undersøgelsen metodisk kun har belyst fortolkninger af de positive oplevelser, og samtidig ikke har belyst ukendte oplevelser, eks. hvor aftagerorganisationen arbejder fortroligt eller ikke har ønsket at deltage grundet dårlige oplevelser. Yderligere erkendes det, at aftagerorganisationer, som ikke har cyberværnepligtige ansat, ikke indgår i undersøgelsen, hvilket udgør en blind vinkel. I praksis har undersøgelsen udelukkende mødt positiv respons i forhold til at sample respondenter; meget sjældent har respondenter ikke ønsket eller ikke tilbudt at være interviewpersoner, og tilsvarende har opbakningen til at medvirke i undersøgelsen været omfattende. Denne positive opbakning og villighed har medført intern undren hos undersøgerne, hvilket muligvis være et resultat af det ene gruppemedlems særlige status internt i Forsvaret. Derudover kan det skyldes, at undersøgelsen er blevet drøftet iblandt aftagere og tidligere cyberværnepligtige. Yderligere kan det være udtryk for, at interviewpersonerne har set denne undersøgelse som en mulighed for et pålideligt talerør, for at ytre deres holdninger indenfor deres interesseområde. Der har været bemærkelsesværdig stor opbakning til at deltage i undersøgelsen, samt at hjælpe med f.eks. sampling. Dette fænomen har manifesteret sig helt fra bruger- til myndighedsniveau. Denne positivitet er forsøgt korrigeret på forskellige måder, f.eks. gennem undersøgelsens metodedesign. Dertil har opbakningen været fordelagtig i forhold til at tilgå visse svært tilgængelige interviewpersoner f.eks. hos CFCS, som ellers er notoriske kendt for at være forbeholdne eller lukkethed. Med dette in mente, så opfattes empiriens subjektivitet stadigvæk som en styrke for undersøgelsens videnskabelse, til dels fordi problemformuleringen understreger, hvordan cyberværnepligtens relevans *opleves*, men også særligt med udgangspunkt i evalueringsperspektivets fokus på aftagerorganisationernes eksplicitte værdi som kilde til at vurdere kvaliteten af cyberværnepligten. Derudover fremhæves undersøgelsens fokus på sporbarhed og transparens som kvalitetskriterie. Al empiri, dens transskriberinger, kodninger, kategorier, osv. er vedlagt som bilag til undersøgelsen, hvilket giver et klart og tydeligt indblik i hvordan og hvorfor empirien behandles. Ligeledes har alle aktivt deltaget i kode- og analysesproces, hvilket understøtter den interne

pålidelighed af undersøgelsens resultater og afhjælper førnævnte bias. Selvom dataens subjektivitet kan skabe risiko for ensartede fortolkninger hos interessenterne, så har undersøgelsen opnået et mætningspunkt i dens kvalitative data. Dertil giver sporbarheden og transparensen i undersøgelsen mulighed for at alle kan tilgå, verificere og genanalysere det datagrundlag, som undersøgelsernes konklusioner beror sig på.

7.4.2 Evalueringstilgang

Undersøgelsens grundlag for at undersøge interessenter som en værdifuld empirikilde, er med afsæt i evalueringsteoriens interaktive rationale. Denne retfærdiggør både hvorfor interessenterne, deres fortolkninger og kontekst, er legitime, men også hvorfor aftagerorganisationerne er særligt gyldige til at vurdere cyberværnepligtens kvalitet. Dette manifesterer sig både i metodiske valg, men også selve analysens opbygning, hvor interessentgrupperne analyseres grupperet i afsnit 5. Valget af en integreret model af elementer fra Interessentmodellen samt BIKVA-modellen, som undersøgelsens evalueringsperspektiv, retfærdiggøres særligt ud fra undersøgelsens begyndelse, hvor intet overblik over relevante interessenter var tilstede. Derfor har en stor del af undersøgelsen været præevaluerende, jf. Interessentmodellen, hvor dét at danne overblik over cyberværnepligtens økosystem har været i fokus. Derimod anerkendes, at andre evalueringstilgange kan benyttes med fordel, særligt som værktøj til at evaluere summativt. F.eks. kan virkningsevaluering bruges, for bedre at vurdere kompleksiteten om *"hvad virker, for hvem, og i hvilken sammenhæng"* (Krogstrup, 2016, s. 107). Virkningsevaluering vil ganske vist bedre kunne etablere forståelse for *effekten* af de cyberværnepligtige som indsats, men har ikke været muligt at udføre fyldestgørende, da grundlaget for en detaljeret programteori ikke har været tilstede i undersøgelsens opstart. Selvom virkningsevaluering vil kunne give en bedre, mere konkret effektforståelse af de cyberværnepligtige, så er det nuværende interaktive rationale brugt, fordi virkningsevaluering ikke er muligt, og fordi evalueringsrationalet er fyldestgørende til at kunne besvare undersøgelsens problemformulering.

Dertil sagt, så kan denne undersøgelse understrege muligheden ved at anvende andre evalueringstilgange, og kan også agere som grundlag for at forstå cyberværnepligtens detaljerede og komplekse bagland af fortolkninger, i forhold til cyberværnepligtens relevans. Dette afkræver tilgengæld bedre målkriterier, med faktiske målbare parametre, samt en bedre beskrivelse af de problemer, som cyberværnepligten skal afhjælpe (Krogstrup, 2016, s. 109). Hertil kan det spekuleres, om mangelfulde målkriterier kan være udtryk for politisk rygdækning, da cyberværnepligten først og fremmest blev politisk bestemt som en forsøgsordning. Ved ikke at fastsætte klare og målbare opfyldelseskriterier for cyberværnepligten, er det svært at holde politiske beslutningstagere ansvarlige for potentielt manglende indfrielse af formel målsætning.

Kapitel 8

Konklusion

Dette afsnit har til formål at besvare undersøgelsens problemformulering i en samlet konklusion, som vist i figur 8.1. Konklusionen tager udgangspunkt i besvarelserne af underspørgsmålene med dertilhørende delkonklusioner, som findes i afsnit 6.1.3, 6.2.3 og 6.3.2, samt diskussionspunkter fra kapitel 7.

Figur 8.1: Konklusionens udgangspunkt og placering

Besvarelsen er baseret på interessentevaluering, som er beskrevet i kapitel 4, med følgende problemformulering:

> *Hvorledes opleves Forsvarets Cyberværnepligt som relevant for at højne IT-sikkerheden ved aftagerorganisationer?*

Forsvarets Cyberværnepligt opleves samlet set som relevant for at højne IT-sikkerheden ved at levere personel med en kombination af kompetencer og personprofil, som er efterspurgt på tværs af private og offentlige aftagerorganisationerne. Cyberværnepligtens relevans er ikke begrænset til Forsvarets myndighedsområde. De cyberværnepligtige bidrager til at højne IT-sikkerhed ved at indgå som en del af en større sikkerhedsstruktur, og derigennem skabe cyberresiliens i aftagerorganisationer. De cyberværnepligtiges bidrag til at øge cyberresiliens er karakteriseret ved at de indgår i en større helhed, og kan derved ikke betragtes som enkeltstående indsatser i aftagerorganisationerne.

Antallet af cyberværnepligtige, som Forsvarets cyberværnepligt årligt uddanner, lever ikke op til forventninger og behov set fra et aftagersynspunkt. Den stigende cybertrussel er direkte medvirkende til yderligere behov for cyberkompetencer. Relevansen af Forsvarets cyberværnepligt påvirkes derfor negativt af, at det årlige antal af cyberværnepligtige er utilstrækkeligt.

Det konkluderes, at intern fastholdelse af cyberværnepligtige i Forsvaret er negativt påvirket af manglende videreuddannelsesmuligheder og karriereveje. Det vurderes, at cyberuddannelse på flere niveauer vil kunne bidrage til øget anvendelse af cyberværnepligtige i Forsvaret. Et længerevarende karriereforløb på flere niveauer, vil bidrage positivt til at øge relevansen af uddannelsen. Her er særligt behov for øgede organisatoriske og ledelsesmæssige kompetencer identificeret. Denne problemstilling er isoleret til Forsvarets eget myndighedsområde.

Den samlede konklusion er baseret på diskussionpunkter samt syntese af de tre underspørgsmål:

Underspørgsmål 1: De cyberværnepligtige vurderes af aftagere at; besidde en god men grundlæggende teknisk forståelse, en tilstrækkelig organisatorisk forståelse til at indgå i en større organisation, men få til ingen ledelsesmæssige kompetencer. Mest centralt opleves cyberværnepligtiges profiler som særligt motiverede og lærenemme indenfor cyberdomænet.
Kombinationen af kompetencer og profil gør de cyberværnepligtige; attraktive, bredt anvendelige og velegnede i aftagerorganisationer.

Underspørgsmål 2: Der er høj grad af overensstemmelse mellem de cyberværnepligtiges tekniske kompetencer, og aftagerorganisationernes tekniske kompetencebehov, hvor særligt netværksforståelse og sikkerhedsanalyse er i fokus. De cyberværnepligtiges organisatoriske kompetencer imødekommer aftagernes kompetencebehov indenfor samarbejde og kommunikation, men vurderes mangelfulde i forhold til risikostyring og framework-forståelse. De cyberværnepligtige besidder få til ingen ledelsesmæssige kompetencer, og imødekommer derfor ikke ledelsesmæssige kompetencebehov. De cyberværnepligtige indtager dog typisk en stilling uden ledelsesansvar. De cyberværnepligtiges motiverede og lærenemme personprofil, stemmer i høj grad overens med aftagernes ønsker og behov.
Det vurderes, at kombinationen mellem de cyberværnepligtiges kompetencer og profil i høj grad imødekommer aftagernes behov i forhold til de typiske jobfunktioner de varetager. De manglende ledelseskompetencer vurderes af aftagerne at afdækkes af andre personalegrupper.

Underspørgsmål 3: Rollen som ambassadør for god IT-sikkerhed manifesterer sig i praksis i meget lav udstrækning. De cyberværnepligtige opleves af aftagerorganisationerne generelt ikke som ambassadører, og besidder ikke funktioner, hvor denne rolle kan praktiseres meningsfyldt. De cyberværnepligtige har i forlængelse heraf svært ved at konkretisere en praktisk udfoldelse af rollen. Ambassadørrollen italesættes internt i Forsvaret som betydningsfuld og vigtig, og afspejles af cyberværnepligtiges egen forventning, men dette kommer ikke til udtryk i praksis ved aftagerorganisationerne, hvilket kan skyldes, at Forsvaret og aftagerorganisationerne fortolker ambassadørrollen forskelligt.

Kapitel 9

Perspektivering

I lyset af undersøgelsens fund og konklusion, vil dette kapitel indlejre undersøgelsens relevans i en bredere sammenhæng.

9.1 Delaftale til Forsvarsforliget 2024-2033

Sideløbende med undersøgelsens udførelse, har forligsparterne i Forsvarsaftalen for 2024-2033 fastsat nye politiske og økonomiske rammer for Forsvaret. Anden delaftale, indgået d. 30 april 2024, nævner eksplicit prioritering af cyberværnepligten:

> *"Aftaleparterne er enige om at følge udviklingen på cyberområdet tæt med henblik på at kunne styrke cyberværnepligten, herunder i forhold til varighed og antallet af værnepligtige i forhold til Forsvarets og det civile samfunds behov. Der gennemføres en evaluering af cyberværnepligten med henblik på, at en styrkelse af cyberværnepligten i højere grad end i dag kan understøtte opgaver inden for eksempelvis beskyttelse af kritisk infrastruktur. Aftaleparterne er endvidere enige om, at en cyberværnepligt efter endt tjeneste skal kunne understøtte den enkeltes videre karriere i både Forsvaret og i det civile."(Forsvarsministeriet, 2024a, s. 10-11).*

Delaftalens eksplicitte omtale af cyberværnepligten, samt behovet for evaluering, understreger denne undersøgelses relevans og anvendelighed. Med fokus i undersøgelsens konklusion om, hvorvidt cyberværnepligten opleves relevant af dens aftagere, koinciderer dette med det aktuelle fokus på cyberområdet og cyberværnepligten. Flere af de områder, som nævnes i aftaleteksten, er identificeret som centrale i denne undersøgelse, og er konkretiseret af aftagerorganisationernes oplevede relevans af cyberværnepligt samt rammesættende interessenter. Det er f.eks. problemstillinger som antallet af cyberværnepligtige og læringsdybde af uddannelsen. Derudover er behovet for at styrke den enkeltes videre karriere, også identificeret i form af manglende videreuddannelsesmuligheder og ansættelsesbarriere. Slutteligt skal nævnes, at en meningsfuld evaluering bør ligge til grund for ændringer i volumen eller format, og at dette bør tage udgangspunkt i behov ved aftagerorganisa-

tionerne, hvadenten de er repræsenteret i kritisk infrastruktur eller internt i Forsvaret. Særligt organisationer i kritisk infrastruktur har udtrykt ønske om øget samarbejde og evt. elevplads eller praktikophold. Dette bekræfter, at undersøgelsen både er relevant, men også anvendelig, da evaluering af cyberværnepligtens relevans kan benyttes som inspiration i den i rammeaftalen omtalte evaluering for at styrke cyberværnepligten.

9.2 Cyberværnepligt på tværs af NATO

Omend undersøgelsen er afgrænset til en dansk kontekst, er den danske cyberværnepligt ikke et enestående fænomen, og lignende indsatser finder sted på tværs af allierede i NATO. Her kan undersøgelsen trække forbindelse til Martin Hurts & Tiia Sõmers (2021) bidrag til at kortlægge specifikke erfaringer og best practices fra cyberværnepligt i de nordiske lande, samt Estland og Schweiz. Selvom der ikke er én fælles definition på cyberværnepligt eller dens udformning på tværs af lande, opfattes cyberværnepligtskonceptet som en mulighed for at styrke nationale cybersecurity-kapabiliteter (Hurt og Sõmer, 2021). Der er enighed om gevinstmulighederne affødt af en national cyberværnepligt, men karakteristika og strukturer varierer. Et eksempel er reservestruktur for cyberværnepligtige i Forsvaret. Dette eksisterer på nuværende tidspunkt ikke i Danmark, som erfaret af de rammesættende interessenter i undersøgelsen. Hertil påpeger Hurt & Sõmer (2021), at en sådan struktur for cyberværnepligtige er under udbygning i Norge og Sverige, og allerede eksisterer i en fuldt funktionel form i Finland og Estland (Hurt og Sõmer, 2021). Det er derved bemærkelsesværdigt, at Danmark som det eneste af landene ikke er i færd med at udbygge en reservestruktur for de cyberværnepligtige i Forsvaret, og dermed afviger fra NATO-allierede. Dog er analyse af genetablering af reservestruktur en del af kommende forsvarsforlig (Forsvarsministeriet, 2024a, s. 10). Der findes ifølge Hurt og Sõmer (2021) forskellig anvendelse af cyberværnepligtige på tværs af partnerlandene. Flere steder ses reel varetagelse af jobfunktioner i landenes Forsvar eller *on-the-job-training* i forbindelse med cyberværnepligten. Her afviger Danmark igen ved ikke at anvende cyberværnepligtige i reelle driftsopgaver udenfor uddannelsesstrukturen ved Føringsstøtteregimentet.

Partnerlandenes cyberværnepligtsuddannelser er af forskellig opbygning, struktur og varighed. De er derfor ikke standardiserede eller sammenlignelige. Dette betyder også, at meritering anvendes forskelligt, hvor nogle lande meriterer mod bachelorniveau på universiteterne, mens der f.eks. i Danmark gives merit for dele af IT-supportuddannelsen.

Interessant er det, at selvom erfaringer fra cyberværnepligten eksisterer i lande lignende Danmark, samarbejder Forsvaret ikke direkte på uddannelsesniveau med andre lande, som også beskrevet i afsnit 5.3.3 vedrørende erfaringsudveksling. Forsvarets nuværende egenevaluering er med udgangspunkt i tilknyttede kurser, men inddrager ikke erfaringer bilateralt, selvom andre lande også har cyberværnepligt med en konstellation, som kan give erfaringer til den danske kontekst. Den manglende erfaringsudveksling og standardisering kan medføre en lavere grad af interoperabilitet, som ellers er et nøglebegreb for NATOs opbygning og sammenhængskraft.

Ordliste

CFCS - Center for Cybersikkerhed

CISOPBTN - Communications and Informations Operationsstøttebataljon

CVPL - Cyberværnepligt(ige)

FE - Forsvarets Efterretningstjeneste

FMN - Forsvarsministeriet

FSR - Føringsstøtteregimentet

GRC - Governance, Risk & Compliance

HBU - Hærens Basisuddannelse

HRU - Hærens Reaktionsstyrkeuddannelse

IP - Interviewperson

SOC - Security Operations Center

Litteratur

Agresti, A. (2018). *Statistical methods for the social sciences, global edition* (5th ed.). London, England: Pearson Education.

Baikloy, E., Praneetpolgrang, P., og Jirawichitchai, N. (2020, August). Development of cyber resilient capability maturity model for cloud computing services. *TEM Journal*, 915–923. Retrieved from http://dx.doi.org/10.18421/TEM93-11 doi: 10.18421/tem93-11

Benyon, D. (2019). *Designing user experience* (4th ed.). London, England: Pearson Education.

Bredgaard, T. (2016). *Evaluering af offentlig politik og administration.* Hans Reitzels Forlag.

Brinkmann, L., Svend. Tanggaard. (2020). *Kvalitative metoder - en grundbog.* Hans Reitzels Forlag.

Bryman, A., Clark, T., Sloan, L., og Foster, L. (2021). *Social research methods, 6th edition.* Oxford University Press.

Christensen, J. G., Christiansen, P. M., og Ibsen, M. (2017). *Politik og forvaltning.* Hans Reitzels Forlag.

European Commision. (2022). *Digital economy and society index 2022.* https://digital-strategy.ec.europa.eu/en/policies/desi. (Besøgt dato: 07/03/2024)

FE. (2020). *EfterretningsmÆssig risikovurdering 2020.* https://www.fe-ddis.dk/da/nyheder/2020/risikovurdering-2020/. (Besøgt dato: 07/03/2024)

FE. (2022). *Udsyn 2022.* https://www.feddis.dk/da/produkter/Risikovurdering/risikovurdering/udsyn-2022/. (Besøgt dato: 07/03/2024)

FE. (2023). *Udsyn 2023.* https://www.fe-ddis.dk/da/produkter/Risikovurdering/risikovurdering/udsyn-2023/. (Besøgt dato: 07/03/2024)

Flyvbjerg, B. (2010). Fem misforståelser om casestudiet. *SSSRN*.

Forsvaret. (2023a). *Forsvarets cyberværnepligt.* ikke-publiserert.

Forsvaret. (2023b). *Rekordmange cyberværnepligtige bliver ved forsvaret.* https://www.forsvaret.dk/da/nyheder/2023/rekordmange-cybervarnepligtige-bliver-ved-forsvaret/. (Besøgt dato: 04/03/2024)

Forsvaret. (2024a). *Føringsstøtteregimentet.* https://www.forsvaret.dk/da/organisation/haeren/Foeringsstoetteregimentet/. (Besøgt dato: 05/03/2024)

Forsvaret. (2024b). *Hæren.* https://www.forsvaret.dk/da/organisation/haeren/. (Besøgt dato: 05/03/2024)

Forsvarsministeriet. (2023). *Analyse af forankringen af cfcs virksomhedsrettede indsats.* https://www.pwc.dk/da/publikationer/2022/pwc-cybercrime-survey-2022.pdf. (Besøgt dato: 07/03/2024)

Forsvarsministeriet. (2024a). *Anden delaftale under forsvarsforliget 2024-2033.* https://www.fmn.dk/globalassets/fmn/dokumenter/nyheder/2024/-anden-delaftale-under-forsvarsforliget-2024-2033-.pdf. (Besøgt dato: 07/03/2024)

Forsvarsministeriet. (2024b). *Departementets organisation.* https://www.fmn.dk/da/ministeriet/forsvarsministeriet/departementets-organisation/. (Besøgt dato: 05/03/2024)

Gioia, D., Corley, K., og Hamilton, A. (2012). Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *SAGE Journal*.

Hurt, M., og Sõmer, T. (2021). Cyber conscription experience and best practice from selected countries. *International Centre for Defence and Security*.

Ingemann, J. H. (2017). *Videnskabsteori for økonomi, politik og forvaltning.* Samfundslitteratur.

Krogstrup, H. K. (2016). *Evalueringsmodeller* (3rd ed.). Hans Reitzels Forlag.

Personalestyrelsen. (2019). *Nu indfører forsvaret cyberværnepligt.* https://www.forpers.dk/da/nyheder/2019/nu-indforer-forsvaret-cybervarnepligt/. (Besøgt dato: 04/03/2024)

PWC. (2022). *Cybercrime survey 2022.* https://www.pwc.dk/da/publikationer/2022/pwc-cybercrime-survey-2022.pdf. (Besøgt dato: 07/03/2024)

Regeringen. (2018a). *Forsvarsforliget 2018-2023.*

Regeringen. (2018b). *National strategi for cyber- og informationssikkerhed.* https://www.regeringen.dk/aktuelt/tidligere-publikationer/national-strategi-for-cyber-og-informationssikkerhed/. (Besøgt dato: 04/03/2024)

Regeringen. (2021). *National strategi for cyber- og informationssikkerhed.* https://www.regeringen.dk/aktuelt/tidligere-publikationer/national-strategi-for-cyber-og-informationssikkerhed-1/. (Besøgt dato: 04/03/2024)

Ross, R., Pillitteri, V., og Dempsey, K. (2022). *Assessing enhanced security requirements for controlled unclassified information.* Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-172A doi: 10.6028/nist.sp.800-172a

Sharma, G., og Bansal, P. (2020). Cocreating rigorous and relevant knowledge. *Academy of Management Journal*.

Venkatesh, V., Brown, S., og Sullivan, Y. (2023). *Conducting mixed-methods research - from classical social sciences to the age of big data and analytics.* Virginia Tech Publishing.

Litteraturstudie

[1] Alessandro Annarelli and Giulia Palombi. “Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework”. In: Sustainability 13.23 (Nov. 2021), p. 13065. issn: 2071-1050. doi: 10 . 3390 / su132313065. url: http://dx.doi.org/10.3390/su132313065.

[2] Gloria Appiah, Joseph Amankwah-Amoah, and Yu-Lun Liu. “Organizational Architecture, Resilience, and Cyberattacks”. In: IEEE Transactions on Engineering Management 69.5 (Oct. 2022), pp. 2218–2233. issn: 1558-0040. doi: 10.1109/tem.2020.3004610. url: http://dx.doi.org/10.1109/TEM.2020.3004610.

[3] Seyedehsaba Bagheri, Gail Ridley, and Belinda Williams. “Organisational Cyber Resilience: Management Perspectives”. In: Australasian Journal of Information Systems 27 (Feb. 2023). issn: 1449-8618. doi: 10. 3127/ajis.v27i0.4183. url: http://dx.doi.org/10.3127/ajis.v27i0.4183.

[4] Ekkachat Baikloy, Prasong Praneetpolgrang, and Nivet Jirawichitchai. “Development of Cyber Resilient Capability Maturity Model for Cloud Computing Services”. In: TEM Journal (Aug. 2020), pp. 915–923. issn: 2217-8309. doi: 10.18421/tem93-11. url: http://dx.doi.org/10.18421/TEM93-11.

[5] Michael Benz and Dave Chatterjee. “Calculated risk? A cybersecurity evaluation tool for SMEs”. In: Business Horizons 63.4 (July 2020), pp. 531–540. issn: 0007-6813. doi: 10.1016/j.bushor.2020.03.010. url: http: //dx.doi.org/10.1016/j.bushor.2020.03.010.

[6] Hugh Boyes. “Cybersecurity and cyber-resilient supply chains”. In: Technology Innovation Management Review 5.4 (Apr. 2015), pp. 28–34. url: http://timereview.ca/article/888.

[7] Elias G. Carayannis et al. “Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience”. In: IEEE Transactions on Engineering Management 68.1 (Feb. 2021), pp. 223–234. issn: 1558-0040. doi: 10. 1109/tem.2019.2909909. url: http://dx.doi.org/10.1109/TEM.2019.2909909.

[8] Juan Francisco Carias et al. “Systematic Approach to Cyber Resilience Operationalization in SMEs”. In: IEEE Access 8 (2020), pp. 174200–174221. issn: 2169-3536. doi: 10.1109/access.2020.3026063. url: http://dx.doi.org/10.1109/ACCESS.2020.3026063.

[9] Juan F. Car´ıas et al. “Cyber Resilience Progression Model”. In: Applied Sciences 10.21 (Oct. 2020), p. 7393. issn: 2076-3417. doi: 10.3390/app10217393. url: http://dx.doi.org/10.3390/app10217393.

[10] Filip Caron. “Obtaining reasonable assurance on cyber resilience”. In: Managerial Auditing Journal 36.2 (Jan. 2019), pp. 193–217. issn: 0268-6902. doi: 10.1108/maj-11-2017-1690. url: http://dx.doi.org/10.1108/MAJ-11-2017-1690.

[11] Se-Ho Choi et al. “Cyber-Resilience Evaluation Methods Focusing on Response Time to Cyber Infringement”. In: Sustainability 15.18 (Sept. 2023), p. 13404. issn: 2071-1050. doi: 10.3390/su151813404. url: http: //dx.doi.org/10.3390/su151813404.

[12] Adrian Davis. “Building Cyber-Resilience into Supply Chains”. In: Technology Innovation Management Review 5.4 (Apr. 2015), pp. 19–27. issn: 1927-0321. doi: 10.22215/timreview/887. url: http://dx.doi.org/10.22215/timreview/887.

[13] Benoˆıt Dupont. “The cyber-resilience of financial institutions: significance and applicability”. In: Journal of Cybersecurity 5.1 (Jan. 2019). issn: 2057-2093. doi: 10.1093/cybsec/tyz013. url: http://dx.doi.org/10.1093/cybsec/tyz013.

[14] Benoˆıt Dupont et al. “The tensions of cyber-resilience: From sensemaking to practice”. In: Computers & Security 132 (Sept. 2023), p. 103372. issn: 0167-4048. doi: 10.1016/j.cose.2023.103372. url: http: //dx.doi.org/10.1016/j.cose.2023.103372.

[15] EU. NIS2 release date — The NIS2 Directive. https://nis2directive.eu/nis2-release-date/. (Accessed on 12/15/2023).

[16] Kjell Hausken. “Cyber resilience in firms, organizations and societies”. In: Internet of Things 11 (Sept. 2020), p. 100204. issn: 2542-6605. doi: 10.1016/j.iot.2020.100204. url: http://dx.doi.org/10.1016/j.iot.2020.100204.

[17] Alexander Kott and Paul Theron. “Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience”. In: IEEE Security & Privacy 18.3 (May 2020), pp. 62–66. issn: 1558-4046. doi: 10.1109/msec. 2020.2983714. url: http://dx.doi.org/10.1109/MSEC.2020.2983714.

[18] Xenofon Koutsoukos. “Systems Science of Secure and Resilient Cyberphysical Systems”. In: Computer 53.3 (Mar. 2020), pp. 57–61. issn: 1558-0814. doi: 10.1109/mc.2020.2966109. url: http://dx.doi.org/10.1109/MC.2020.2966109.

[19] In Lee. “Cybersecurity: Risk management framework and investment cost analysis”. In: Business Horizons 64.5 (Sept. 2021), pp. 659–671. issn: 0007-6813. doi: 10 . 1016 / j . bushor . 2021 . 02 . 022. url: http : //dx.doi.org/10.1016/j.bushor.2021.02.022.

[20] John Loonam et al. “Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective”. In: IEEE Transactions on Engineering Management 69.6 (Dec. 2022), pp. 3757–3770. issn: 1558-0040. doi: 10.1109/ tem.2020.2996175. url: http://dx.doi.org/10.1109/TEM.2020.2996175.

[21] Georgia Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis. “Smart Airport Cybersecurity: Threat

Mitigation and Cyber Resilience Controls". In: Sensors 19.1 (Dec. 2018), p. 19. issn: 1424-8220. doi: 10.3390/ s19010019. url: http://dx.doi.org/10.3390/s19010019.

[22] Logan O. Mailloux and Michael Grimaila. "Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce". In: IT Professional 20.3 (May 2018), pp. 23–30. issn: 1941-045X. doi: 10.1109/ mitp.2018.032501745. url: http://dx.doi.org/10.1109/MITP.2018.032501745.

[23] Florian Maurer and Albrecht Fritzsche. "Layered structures of robustness and resilience: ¡scp¿Evidence¡/scp¿ from cybersecurity projects for critical infrastructures in ¡scp¿Central Europe¡/scp¿". In: Strategic Change 32.6 (Oct. 2023), pp. 195–208. issn: 1099-1697. doi: 10.1002/jsc.2559. url: http://dx.doi.org/10.1002/jsc.2559.

[24] Gemma Moore et al. "A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland". In: (May 2023). doi: 10.21203/rs.3.rs-2534270/v1. url: http://dx.doi.org/10.21203/rs.3.rs-2534270/v1.

[25] Martina Neri, Federico Niccolini, and Luigi Martino. "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment". In: Information & Computer Security (July 2023). issn: 2056-4961. doi: 10.1108/ics-05-2023-0084. url: http://dx.doi.org/10.1108/ICS-05-2023-0084.

[26] News Releases — NIST. https://www.nist.gov/cyberframework/newsroom/news-releases. (Accessed on 12/15/2023).

[27] Eline Punt et al. "Navigating cyber resilience in seaports: challenges of preparing for cyberattacks at the Port of Rotterdam". In: Digital Policy, Regulation and Governance 25.4 (May 2023), pp. 420–438. issn: 2398-5038. doi: 10.1108/dprg-12-2022-0150. url: http://dx.doi.org/10.1108/DPRG-12-2022-0150.

[28] Rishabh Rajan et al. "Developing a modified total interpretive structural model (M-TISM) for organizational strategic cybersecurity management". In: Technological Forecasting and Social Change 170 (Sept. 2021), p. 120872. issn: 0040-1625. doi: 10.1016/j.techfore.2021.120872. url: http://dx.doi.org/10.1016/j.techfore.2021.120872.

[29] ResearchAndMarkets. Cyber Security Market by Component (Software, Hardware, and Services) Software (IAM Encryption and Tokenization, and Other Software), Security Type, Deployment Mode, Organization Size, Vertical and Region - Global Forecast to 2027. 20/12/2023. 2022. url: https : / / www . researchandmarkets . com / reports / 5651552 / cyber - security - market - by - component - software ? utm _ source = BW & utm _ medium = PressRelease & utm _ code = tbgxqv & utm _ campaign = 1754451+ - +Global + Cyber+Security+Market+Report+(2022+to+2027)+-+IoT+Security+to+Play+a+Vital+Role+in+ Cybersecurity&utm_exec=jamu273prd.

[30] Retsinformation. Lov om net- og informationssikkerhed for domænenavnssystemer og visse digitale tjenester. 20/12/2023. 2018. url: https://www.retsinformation.dk/eli/lta/2018/436.

[31] Ron Ross, Victoria Pillitteri, and Kelley Dempsey. Assessing enhanced security requirements for controlled unclassified information. Mar. 2022. doi: 10.6028/nist.sp.800-172a. url: http://dx.doi.org/10.6028/NIST.SP.800-172A.

[32] Daniel S. Schabacker et al. "Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience". In: Frontiers in Bioengineering and Biotechnology 7 (Mar. 2019). issn: 2296-4185. doi: 10.3389/fbioe.2019.00061. url: http://dx.doi.org/10.3389/fbioe.2019.00061.

[33] International Organization for Standardization. ISO/IEC 27001:2022. 20/12/2023. 2022. url: https://www.iso.org/standard/27001.

[34] William Steingartner, Darko Galinec, and Andrija Kozina. "Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model". In: Symmetry 13.4 (Apr. 2021), p. 597. issn: 2073-8994. doi: 10.3390/sym13040597. url: http://dx.doi.org/10.3390/sym13040597.

[35] Mariela Tapia, Pablo Thier, and Stefan G¨oßling-Reisemann. "Building resilient cyber-physical power systems: An approach using vulnerability assessment and resilience management". In: TATuP - Zeitschrift f¨ur Technikfolgenabsch ¨atzung in Theorie und Praxis 29.1 (Apr. 2020), pp. 23–29. issn: 2568-020X. doi: 10.14512/ tatup.29.1.23. url: http://dx.doi.org/10.14512/tatup.29.1.23.

[36] Peter R. J. Trim and Yang-Im Lee. "Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience". In: Big Data and Cognitive Computing 6.4 (Oct. 2022), p. 110. issn: 2504-2289. doi: 10.3390/bdcc6040110. url: http://dx.doi.org/ 10.3390/bdcc6040110.

[37] Peter R.J. Trim and Yang-Im Lee. "The Global Cyber Security Model: Counteracting Cyber Attacks through a Resilient Partnership Arrangement". In: Big Data and Cognitive Computing 5.3 (July 2021), p. 32. issn: 2504-2289. doi: 10.3390/bdcc5030032. url: http://dx.doi.org/10.3390/bdcc5030032.

[38] Elinor Tsen, Ryan K L Ko, and Sergeja Slapnicar. "An exploratory study of organizational cyber resilience, its precursors and outcomes". In: Journal of Organizational Computing and Electronic Commerce 32.2 (Apr. 2022), pp. 153–174. issn: 1532-7744. doi: 10.1080/10919392.2022.2068906. url: http://dx.doi.org/10. 1080/10919392.2022.2068906.

[39] Betsy Uchendu et al. "Developing a cyber security culture: Current practices and future needs". In: Computers & Security 109 (Oct. 2021), p. 102387. issn: 0167-4048. doi: 10.1016/j.cose.2021.102387. url: http: //dx.doi.org/10.1016/j.cose.2021.102387.

[40] J Webster and R.T. Watson. "Analyzing the Past to Prepare for the Future: Writing a Literature Review". In: MIS Quarterly 26.2 (June 2002), pp. xiii–xxiii.

[41] Joost F Wolfswinkel, Elfi Furtmueller, and Celeste P M Wilderom. "Using grounded theory as a method for rigorously reviewing literature". In: European Journal of Information Systems 22.1 (Jan. 2013), pp.

45–55. issn: 1476-9344. doi: 10.1057/ejis.2011.51. url: http://dx.doi.org/10.1057/ejis.2011.51.

Bilag

Alle bilag kan findes i bilagsmappen, hvor hvert hovedbilag er inddelt alfabetisk og indeholder respektive underbilag.

[A] Transskriberinger

[A1] transskription af interviewperson 1 (IP 1)
Se fil: Bilag_A1_IP1_Rammesættende_120224.pdf

[A2] transskription af interviewperson 2 (IP 2)
Se fil: Bilag_A2_IP2_Rammesættende_110324.pdf

[A3] transskription af interviewperson 3 (IP 3)
Se fil: Bilag_A3_IP3_Rammesættende_260324.pdf

[A4] transskription af interviewperson 4 (IP 4)
Se fil: Bilag_A4_IP4_CivilAftager_120324.pdf

[A5] transskription af interviewperson 5 (IP 5)
Se fil: Bilag_A5_IP5_CivilAftager_130324.pdf

[A6] transskription af interviewperson 6 (IP 6)
Se fil: Bilag_A6_IP6_CivilAftager_130324.pdf

[A7] transskription af interviewperson 7 (IP 7)
Se fil: Bilag_A7_IP7_CivilAftager_210324.pdf

[A8] transskription af interviewperson 8 (IP 8)
Se fil: Bilag_A8_IP8_MilitærAftager_180324.pdf

[A9] transskription af interviewperson 9 (IP 9)
Se fil: Bilag_A9_IP9_MilitærAftager_220324.pdf

[A10] transskription af interviewperson 10 (IP 10)
Se fil: Bilag_A10_IP10_CivilAftager_270324.pdf

[B] Kodning af transskriberinger

Rammesættende:

[B1] Kodning af tema "Cybersikkerhed i din organisation"
Se mappe: Bilag_B1_Cybersikkerhed_i_din_organisation

[B2] Kodning af tema "Cyberuddannelse i Forsvaret"
Se mappe: Bilag_B2_Cyberuddannelse_i_Forsvaret

[B3] Kodning af tema "Forsvarets cyberværnepligt"
Se mappe: Bilag_B3_Forsvarets_Cyberværnepligt

[B4] Kodning af tema "Nationalt sikkerhedsansvar"
Se mappe: Bilag_B4_Nationalt_sikkerhedsansvar

Aftagere:

[B5] Kodning af tema "Aftager"
Se mappe: Bilag_B5_Aftager

[B6] Kodning af tema "Ambassadørrolle"
Se mappe: Bilag_B6_Ambassadørrolle

[B7] Kodning af tema "Andet"
Se mappe: Bilag_B7_Andet

[B8] Kodning af tema "Cyberværnepligten"
Se mappe: Bilag_B8_Cyberværnepligten

[B9] Kodning af tema "Nationalt sikkerhedsansvar"
Se mappe: Bilag_B9_Nationalt_sikkerhedsansvar

[B10] Kodning af tema "Uddannelse"
Se mappe: Bilag_B10_Uddannelse

[C] Kodning af klyngedata og observationsdata

[C1] Kodning af klyngeinterview
Se fil: Bilag_C1_Kodning_af_klyngeinterview.pdf

[C2] Kodning af observationsstudie
Se fil: Bilag_C2_kodning_af_observationsdata.pdf

[C3] Observationsdata (rådata)

Se fil: Bilag_C3_Observationsdata (rådata).xlsx

[D] Interviewguides

[D1] Interviewguide til civile og militære aftagere

Se fil: Bilag_D1_Interviewguide_civile_og_militære_aftagere.pdf

[D2] Interviewguide til IP10

Se fil: Bilag_D2_Interviewguide_IP10.pdf

[D3] Interviewguide til IP1

Se fil: Bilag_D3_Interviewguide_IP1.pdf

[D4] Interviewguide til IP2

Se fil: Bilag_D4_Interviewguide_IP2.pdf

[D5] Interviewguide til IP3

Se fil: Bilag_D5_Interviewguide_IP3.pdf

[D6] Interviewguide til Klyngeinterview

Se fil: Bilag_D6_Klynge_interviewguide.pdf

[E] Spørgeskema

[E1] Spørgeskema til nuværende cyberværnepligtige (uden besvarelser)

Se fil: Bilag_E1_nuværende_cyberværnepligtige_uden_besvarelser.pdf

[E2] Spørgeskema til nuværende cyberværnepligtige (med besvarelser)

Se fil: Bilag_E2_nuværende_cyberværnepligtige_med_besvarelser.csv

[E3] Spørgeskema til tidligere cyberværnepligtige (uden besvarelser)

Se fil: Bilag_E3_tidligere_cyberværnepligtige_uden_besvarelser.pdf

[E4] Spørgeskema til tidligere cyberværnepligtige (med besvarelser)

Se fil: Bilag_E4_tidligere_cyberværnepligtige_med_besvarelser.csv

[E5] Spørgeskema til aftagerorganisationer (uden besvarelser)

Se fil: Bilag_E5_aftager_uden_besvarelser.pdf

[E6] Spørgeskema til aftagerorganisationer (med besvarelser)

Se fil: Bilag_E6_aftager_med_besvarelser.csv

[F] Behandling af kvantitative data

[F1] Beskrivelse af kvantitativ databehandling i undersøgelsen.
Se fil: Bilag_F1_Behandling_af_kvantitativ_data.pdf

[F2] Datafigurer til de nuværende cyberværnepligtige.
Se mappe: Bilag_F2_Nuværende_cyberværnepligtige_data_figurer

[F3] Datafigurer til de tidligere cyberværnepligtige.
Se mappe: Bilag_F3_Tidligere_cyberværnepligtige_data_figurer

[F4] Datafigurer til aftagerorganisationerne.
Se mappe: Bilag_F4_Aftager_data_figurer

[G] Dokumenter

[G1] Præsentation fra introduktionsmøde med Føringsstøtteregimentet
Se fil: Bilag_G1_Præsentation_intromøde.pdf

[G2] Kompetencekort for cyberværnepligtsuddannelsen
Se fil: Bilag_G2_Kompetencekort_for_cyberværnepligten.pdf

[G3] Uddannelsesbeskrivelse for cyberværnepligten
Se fil: Bilag_G3_Uddannelsesbeskrivelse_cyberværnepligten.pdf

[H] Analyse af øvrige temaer

[H1] Analyse af øvrige teamer fra analysen
Se fil: Bilag_H1_Analyse_af_temaer.pdf

[I] Kvalitative metoder

[I1] Bilag som indeholder kvalitative metoder fra metode afsnittet
Se fil: Bilag_I1_kvalitative_metoder.pdf

[I2] Figur fra mixed methods afsnittet
Se fil: Bilag_I2_Mixed_method.png

[J] Temaer fra teoretisk perspektiv

[J1] Bilag indeholdende de fulde tabeller med temaer fra det teoretiske perspektiv
Se fil: Bilag_J1_tabeller_teoretisk_perspektiv.pdf

[K] Litteraturstudie

[K1] Bilag indeholdende litteraturstudie om "Ledelse af Cyberresiliens I Organisationer"
se fil: Bilag_K1_Ledelse_af_cyberresiliens.pdf

[L] Farvekoder

[L1] Bilag indeholdende farvekoder brugt på empiriens temaer til analysen
se mappe: Bilag_L1_Aftagere_farvekoder & Bilag_L2_Rammesættende_farvekoder