Nr. _____ av _____


# Sjøkrigsskolen

## Bacheloroppgave

Maritim Cybersikkerhet

*–Teknologiens bakside i et operativt perspektiv–*

Av

Johannes Haug Steinholt & Ola Namtvedt

Levert som en del av kravet til graden:

BACHELOR I MILITÆRE STUDIER MED FORDYPNING I NAUTIKK

Innlevert: Mai 2018

**Godkjent for offentlig publisering**

# Publiseringsavtale

## En avtale om elektronisk publisering av bachelor/prosjektoppgave

Kadetten(ene) har opphavsrett til oppgaven, inkludert rettighetene til å publisere den.

Alle oppgaver som oppfyller kravene til publisering vil bli registrert og publisert i Bibsys Brage når kadetten(ene) har godkjent publisering.

Oppgaver som er graderte eller begrenset av en inngått avtale vil ikke bli publisert.

| | | |
|---|---|---|
| Vi gir herved Sjøkrigsskolen rett til å gjøre denne oppgaven tilgjengelig elektronisk, gratis og uten kostnader | [X] Ja | [ ] Nei |
| Finnes det en avtale om forsinket eller kun intern publisering? (Utfyllende opplysninger må fylles ut)<br><br>Hvis ja: kan oppgaven publiseres elektronisk når embargoperioden utløper? | [ ] Ja<br><br>[-] Ja | [X] Nei<br><br>[-] Nei |

# Plagiaterklæring

Vi erklærer herved at oppgaven er vårt eget arbeid og med bruk av riktig kildehenvisning. Vi har ikke nyttet annen hjelp enn det som er beskrevet i oppgaven. Vi er klar over at brudd på dette vil føre til avvisning av oppgaven.

**Dato: 28-05-2018**

| | |
|---|---|
| Ola Namtvedt | |
| Kadett navn | Kadett, signatur |
| Johannes Haug Steinholt | |
| Kadett navn | Kadett, signatur |

# Forord

I likhet med barneoppdragelse, skipsbygging og whiskey-destillering starter ofte gode ting i det små og utvikler seg i retninger man ikke kunne forestille seg. Resultatet blir ofte helt annerledes i forhold til den originale visjonen. Idéen til denne oppgaven ble til over en halvliter øl med tilhørende skitprat og gikk ut på å plante et virus som skulle senke Marinens fartøyer. Idéen modnet med tiden og etter mangfoldige timer med konsekvensutredning, prøving, feiling, utsettelse av deadlines og vennligsinnet krangling endte vi opp med ca. 60 sider ymse tekst, tabeller, minnerike erfaringer og et resultat totalt ulikt det vi hadde sett for oss.

Denne oppgaven ble skrevet i den hensikt å belyse det vi oppfattet som et stadig økende problem ved en militær avdeling som i våre øyne ikke fulgte med i den teknologiske utviklingen på en sikker måte. For å klare å gjennomføre de undersøkelser og analyser krevd for å belyse dette temaet fikk vi uvurderlig hjelp fra gode støttespillere ved Sjøkrigsskolen og i Sjøforsvaret.
Vi ønsker å rette en stor takk til Orlogskaptein Petter Lunde og Kapteinløytnant Odd Sveinung Hareide ved Navkomp for faglig støtte og sparring under oppstartsfasen av denne oppgaven i den hensikt å få oss på rett kurs.
En stor takk til Fenrik Kristian Mathisen i Ubåtvåpenet som stilte opp på dugnad for å assistere to styrepinner i søken etter riktig programvare. Vi vil også takke Visekonstabel Martin Frotvedt for å raskt og effektivt gjøre de tekniske forberedelsene som var påkrevd for at vi skulle kunne gjennomføre eksperimentet vårt.
Operativ Marine i Kull Uredd fortjener en takk for å ha stilt velvillig opp som respondenter i eksperimentet vårt, som oppgaven ikke kunne vært foruten.

Til sist vil vi rekke en stor takk til Jan Otto Jacobsen som med stor interesse og iver har vært vår mentor og veileder gjennom denne oppgaven. Han vil bli dypt savnet ved Sjøkrigsskolen og vi ønsker han all lykke og hell ved Universitet i Stavanger.

Bergen, Sjøkrigsskolen, 28-05-2018

# Abstract

I lys av den enorme utviklingen som skjer innen datakraft og IKT-teknologi blir bruken av datasystemer en stadig mer omfattende del av hverdagen. Det blir som følge av dette desto viktigere å sikre informasjonssystemer mot potensielle trusler, blant annet gjennom konkret utdanning av systemets operatører: mennesket.
På Sjøkrigsskolen foregår omfattende utdanningsløp integrert med bruken av graderte og ugraderte systemer. Tjeneste i Sjøforsvaret innebærer også bruk av tilsvarende systemer. Det blir derfor relevant å observere og eksperimentere på hvordan kulturen for bruk av graderte og ugraderte systemer foregår på Sjøkrigsskolen i den hensikt å fokusere, forbedre og utvikle denne kulturen.

Vi utførte et kvasi-eksperiment på en enkelt skoleklasse på skolen med målsetningen om å studere hvilken effekt innføring av en operasjonsprosedyre som sikkerhetsrutine vil ha på et slikt utvalg. Funnene viser i stor grad at innføringen av prosedyren har liten effekt og at grunnen til dette kan være avhengig av tredjepartsfaktorer som på mange måter kan utgjøre det som er Sjøkrigsskolens datasikkerhetskultur. Med andre ord er det en kompleks situasjon vi er ute for og det å endre atferden i en etablert kultur viste seg vanskeligere å studere enn forventet.

Med fokus på maritim cybersikkerhet er det tydelig at det kan eksistere betydelige sikkerhetshull og trusler slik som datasikkerhetskulturen på Sjøkrigsskolen er per i dag. Vi stiller derfor spørsmålet om dette må tas tak i av skolens ledelse i form av en strategiendring, om kompetansemiljøer rundt cybersikkerhet på bygges opp eller om kadettmassen er roten til utfordringen.

# Innholdsfortegnelse

## Figurliste



## Tabeller



## Forkortelser

| | |
|---|---|
| AV | Anti-Virus |
| MCS | Maritime Cyber Security |
| SKSK | Sjøkrigsskolen |
| PS | Planning Station/planleggingsstasjon |
| SOP | Standard/stående operasjonsprosedyre |
| O1 | Observasjon 1 |
| X | Behandling |
| O2 | Observasjon 2 |

## Begreper og uttrykk

| | |
|---|---|
| NAVKOMP | Navigasjonskompetansesenter. Avdeling for navigasjonsutdanning og -mønstring i marinen. Underlagt KNM Tordenskjold på Haakonsvern, men befinner seg på Sjøkrigsskolen |
| Navlab | Navigasjonslaboratoriet. Laboratorium for testing av navigasjonssystemer, samt planlegging av ruter før seilas. Underlagt Navkomp. |
| Teksim | Teknologisimulator. Simulator for drift av teknisk utstyr om bord, samt planlegging av ruter før seilas. Underlagt Navkomp, og befinner seg i Navsim. |
| Navsim | Navigasjonssimulator. Simulatoranlegg for trening på navigasjon og skipshåndtering. Brukes av kadetter og marinen ellers for trening og utdanning. Underlagt Navkomp og ligger på Sjøkrigsskolen |
| OM-2 | Operativ Marine, 2. klasse. Linje ved Sjøkrigsskolen med hovedfag navigasjon og ledelse. |
| Seilingsgruppe | En fag-gruppe kadettene jobber sammen i. Gruppen består av 3-4 kadetter med den hensikt at de skal jobbe sammen om planlegging og gjennomføring av navigasjonsøvelser, samt fungere sammen som et bro-team både i simulator og på skolefartøyene. |
| Open source | Open source informasjon/open source intelligence (OSINT) er informasjon og etterretning som kan innhentes fra åpne kilder, særlig fra massemedia og sosiale media. Dette er gjerne facebookstatuser, bilder på instagram, meldinger på twitter og all annen informasjon som er åpent tilgjengelig. |
| Pretest | I forbindelse med et forsøk eller eksperiment foretar man en pretest som et sammenligningsgrunnlag før man innfører en behandling. |
| Behandling | Begrep i forbindelse med eksperimenter og forsøk. Behandling innføres vanligvis etter en form for pretest i den hensikt å studere en endring eller en effekt hos et utvalg. Et eksempel på |

| | |
|---|---|
| | behandling kan være alt fra et legemiddel til en handling eller en metode. |
| Posttest | Etter en behandling er innført som del av et eksperiment, utføres en posttest for å måle eventuelle forskjeller. |

# 1 Innledning

April 2014: En russisk Su-24 Fencer flyr gjentatte ganger over USS Donald Cook i Svartehavet mens den gjennomfører engasjementsdriller. Om bord på den amerikanske jageren går angivelig alle angrepssystemene i svart.

Januar 2017: Sivile passasjerfly fra Widerøes Flyveselskap rapporterer om flere hendelser med bortfall av GPS-signalet i Finnmark. Den norske stat kobler i ettertid hendelsen til en russisk øvelse med elektronisk krigføring.

Ved begge hendelsene er tilstedeværelsen av elektronisk krigføring kilde til usikkerhet rundt hva som egentlig skjedde. Alle parter sitter dermed igjen med hver sine tolkninger av hendelsene og dette kan bli en kilde til konflikt og økt spenning. Nye typer krigføring gir uante muligheter, men også uante trusler i fremtidens virkelighetsbilde.

## 1.1 Bakgrunn

I dagens samfunn spiller teknologi en stadig større rolle i hvordan livene våre og samfunnet kommuniserer og knyttes sammen. Teknologien gir oss muligheten til å utvikle oss og kommunisere raskere enn noen. Mulighetene teknologien gir oss er enorme og det samme kan også sies om farene.

Med rask utvikling følger alltid en viss usikkerhet overfor ukjente problemer. Innenfor datasikkerhet er dette et stadig voksende problem; både den offensive og den defensive part er med på en veldig volatil og brutal utvikling som gjør det vanskelig for alle aktører å henge med.

Også i Forsvaret er vi i økende grad aktører på den datasikkerhetsmessige arenaen. Det kan argumenteres for at den eneste måten å skulle garantere sikkerhet mot dataangrep er å isolere seg helt fra bruk av datasystemer og holde seg til analoge og manuelle systemer. I dagens forsvar er dette nærmest umulig da vi i stor grad er knyttet sammen og fullstendig avhengig av datasystemer. Slik oppstår derfor behovet for god sikkerhet rundt disse systemene.

På lik linje med tekniske sikkerhetsbarrierer inngår også menneskene som bruker systemet i denne kjeden. Mennesker både opererer og forvalter systemene. Dette betyr at menneskers handlemåter også kan inngå som en grunnleggende sikkerhetsrisiko. Systemene våre er sammensatt av graderte og ugraderte delsystemer og data må ofte overføres mellom disse på en sikker måte. Kunnskaper, ferdigheter og opplæring om hva som kan kobles sammen og hvordan det gjøres ordentlig er derfor viktig.

Denne problemstillingen går igjen på flere steder i Marinen, for eksempel ved overføring av navigasjonsruter fra planleggingsstasjoner på land til kartmaskinene ombord. Kartmaskiner ombord er ikke koblet til internett og vil derfor ikke automatisk oppdaterte anti-virusdatabaser og nye sikkerhetsfunksjoner for å takle nye trusler. Dette kan gjøre systemene sårbare hvis systemene først blir kompromittert. Risikoen kan derfor senkes ved at operatører manuelt scanner overføringsenheter for skadelig programvare før tilkobling til kartmaskiner ombord (Wråli, 2017).

## 1.2 Problemstilling

God datasikkerhet krever altså innsats og gode rutiner hos menneskene som opererer systemene. Vi kan da stille spørsmålet: hvilken utdanning gir Sjøkrigsskolen dagens kadetter innen datasikkerhet? For å belyse dette spørsmålet ønsker vi å drøfte følgende problemstilling i vår bachelor-oppgave:

> *Hvilken effekt har en konkret operasjonsprosedyre på kadetters handlemønster innen datasikkerhet under planleggingsfasen før en maritim øvelse?*

## 1.3 Mål

Hovedmålet med denne oppgaven kan deles i flere delmål. Som utgangspunkt er målet å studere holdningene til datasikkerhet hos et utvalg kadetter ved Sjøkrigsskolen. Videre ut ifra dette blir det da naturlig å kartlegge hvordan enkle datasikkerhetsrutiner foregår på skolen og hvordan de eventuelle prosedyrene er utformet. Vi ønsker med andre ord å se på hvilke handlemønstre som eksisterer hos kadettene. Til slutt blir målet med oppgaven å gi Sjøkrigsskolen og Navigasjonskompetansesenteret data, resultater og et eventuelt forslag til rutiner/prosedyrer som kan brukes på skolen og bidra til konstruktive endringer i skolens tilnærming til datasikkerhet. Ikke minst er det viktig for oss å bidra til at datasikkerhetsopplæringen ved skolen utvikles, suppleres og forbedres. Dette for at fremtidens offiserer skal ta med seg det vi anser for å være sunne holdninger innen datasikkerhet ut i tjeneste i Sjøforsvaret.

## 1.4 Avgrensninger

I denne oppgaven tar vi i hovedsak for oss datasikkerhetskultur hos andreårselevene ved linjen Operativ Marine på Sjøkrigsskolen. Det betyr at vi ønsker å kun studere kadettene i klassen OM-2. Klassen har et øvingsprogram innen navigasjon som gir et godt grunnlag for empiriske undersøkelser. Oppgavens drøftingsgrunnlag vil derfor kun omhandle empiriske observasjoner fra denne klassen.

I oppgaven er det også kun observasjoner av kadettenes bruk av lagringsenheter på spesifikke datamaskiner i et gitt tidsrom på 3 måneder som vil undersøkes. Det finnes sikkerhetsaspekter utenom det vi velger å studere, men i oppgavens formål anser vi det som mest relevant å begrense oss til gitt maskinvare. Antall og omfang av dette vil redegjøres for ytterligere i kapittel 3.

## 1.5 Struktur og oppbygging

Denne oppgaven er delt i 6 hovedkapitler med diverse underkapitler.

Kapittel 1 tar for seg innledning, bakgrunn for oppgaven og problemstilling, samt overordnede mål for oppgaven.

Kapittel 2 redegjør for hvilke tidligere tekster og teorigrunnlag vi baserer oss på, og beskriver i detalj de teorier som er relevant for oppgavens drøftingsdel.

Kapittel 3. Vi går gjennom metoden og metodedesignet vi har utviklet for å kunne utforske og drøfte problemstillingen vi har valgt. Alle detaljer rundt metodikk og eksperimentdesign vil gjennomgås her.

Kapittel 4 og 5 tar for seg resultat- og drøftingsdelen av oppgaven. Her vil vi gå gjennom resultatene fra undersøkelsen, samt de forskjellige problemstillingene rundt resultatene vi har oppnådd og forsøke å danne et grunnlag for å konkludere oppgaven.

Kapittel 6. Til slutt vil vi konkludere funnene og drøftingen rundt problemstillingen.

# 2 Teori

Dette kapittelet vil omtale relevant teori omkring temaet datasikkerhet og cybersikkerhet, samt redegjøre for hovedbegreper og underbegreper. Det vil redegjøres for hva vi legger i begrepet Maritim Cybersikkerhet samt sampspillet mellom mennesket og datasystem. Vi vil videre redegjøre for cybsersikkerhet i en organisasjon med fokus på trusler, modeller og forsvarskonsepter. Til slutt vil det presenteres relevant teori rundt de ulike trekkene ved et kvasi-eksperiment som undersøkelsesform.

## 2.1 Maritim Cybersikkerhet

Maritim cybersikkerhet er i hovedsak en sammenslåing av to begreper: Maritim sikkerhet og cybersikkerhet. Maritim sikkerhet omfavner de fysiske aspektene når det gjelder risiko og sikkerhet i forbindelse med sjøfart og virke på havet (Hareide, Jøsok, Ostnes, Helkala, & Lund, 2018, s. 2). Eksempelvis er sjøfarten et grunnleggende farlig arbeid tilknyttet fare og risiko der mennesker bemanner fartøy og maskineri enten for å frakte last, bedrive fiske eller manøvrere krigsskip. Det er i disse sammenhengene mulighet for skade på personell og maskineri og sikkerhetstiltak er derfor nødvendig for å motvirke potensielt skadeomfang.

Cybersikkerhet omfatter informasjonssikkerhet og hvordan informasjonens konfidensialitet, integritet og tilgjengelighet blir ivaretatt (Departementene, 2012, s. 10). Cyber-domenet er derfor grunnleggende ulikt det fysiske domenet og baserer seg rundt nettverk, programvare og maskinvare (Hareide, Jøsok, Ostnes, Helkala, & Lund, 2018, s. 2). Dette utelukker derimot ikke at det ikke kan påvirke den virkelige verden. Det er mulig å utnytte sårbarheter i cyber-domenet som kan gi store, alvorlige og kostbare konsekvenser i den fysiske verden enten det gjelder sabotasje og påvirkning av et industrielt anlegg eller mulig manipulasjon av GPS-systemene ombord på et krigsfartøy (Goward, 2017).

Dagens maritime krigføring er i største grad avhengig av komplekse datasystemer og høyteknologisk utstyr som må samhandle for at en maritim våpenplattform skal kunne manøvrere og levere våpen eller fylle en støttefunksjon. Maritim cybersikkerhet vil i denne oppgavens formål defineres som all type beskyttelse av datasystemer på en maritim militær plattform mot trusler som kan gå utover systemets integritet og tilgjengelighet (Hareide, Jøsok, Ostnes, Helkala, & Lund, 2018).

## 2.2 Mennesket

Til tross for at et maritimt krigsfartøy er bygd opp rundt datasystemer og høyteknologisk utstyr er det likevel mennesker som skal betjene, operere og forvalte teknologien. Menneskets natur og oppførsel blir derfor sentral når det kommer til maritim cybersikkerhet da operatørenes handlinger kan være en kritisk kilde til et datasystems sårbarhet (Fitton, Prince, Lacy, & Germond, 2015, s. 22). PhD-stipendiat Oliver Fitton et al. beskriver i sin artikkel *The Future of Maritime Cyber Security* at mennesker som operatører av et datasystem medfører betydelig risiko for datasikkerheten. Han peker blant annet på økning i mengde, utbredelse og tilgjengelighet av open source-informasjon i dagens samfunn. I maritim kontekst gjelder dette for eksempel AIS som gratis og lett tilgjengelig viser posisjon, kurs og fartsinformasjon til all kommersiell skipstrafikk verden over. I tillegg er betydelige mengder informasjon om enkeltpersoner tilgjengelig via sosiale medier. Før var slik informasjon mye vanskeligere å få tak i, mens i dag er dette tilgjengelig på internett. Operatører med hensikt og vilje til å skade og utføre angrep kan dermed samle store mengder informasjon på kort tid (Fitton, Prince, Lacy, & Germond, 2015, s. 16).

Trusler kan deles i to kategorier. En innsidetrussel vil naturlig befinne seg inne i egen organisasjon og være en stor trussel med tanke på lekkasjer og kompromittering av informasjon. En utsidetrussel vil på sin side kunne skade ved å forstyrre og legge press på enkeltindivider eller deler av organisasjonen og samtidig holde seg anonym (Fitton, Prince, Lacy, & Germond, 2015, s. 22).
Fitton skriver også at utvidet fokus på utdanning og prosedyrer bør være obligatorisk i dagens informasjonssamfunn og bør likestilles i maritim sektor på lik linje med vanlig HMS-relatert arbeid (Fitton, Prince, Lacy, & Germond, 2015, s. 21). Operatører i et maritimt miljø, på et fartøy eller en installasjon vil kunne oppleve angrep gjennom sosiale medier eller andre digitale kanaler og bør derfor vite nøyaktig hva han/hun bør gjøre hvis så skjer. Her argumenteres det for at etablerte prosedyrer ved angrep, enten kjente eller ukjente, bør være til stede i en maritim organisasjon.

Under Den Norske Atlanterhavskomités kurs i internasjonal politikk ved Sjøkrigsskolen i april 2018 uttalte seniorforsker og spesialrådgiver i Cyberforsvaret, Hanne Røislien, at «nordmenn vil kunne, men ønsker ikke å lære» når hun snakket om cybersikkerhet i det norske samfunn. Her argumenterte hun sterkt for at den teknologiske utviklingen går

langt raskere enn menneskers utdanning innen datakunnskap og at det er et stort gap der som må fylles (Røislien, 2018).

### 2.2.1 Ansvarliggjøring og kompetanse

Pensjonert Kommandør i US Navy L. David Marquet argumenterer tungt for at ansvarliggjøring av personell med tilstrekkelig kompetanse på fagfeltet sitt er den beste måten å drifte en organisasjon på (Marquet, 2012). Dette kan gjelde alt fra prosedyrer, arbeidsoppgaver, feilsøking og operasjoner over lang tid. For at personell skal gjennomføre jobben sin på best måte er man avhengig av at de vet hva de skal gjøre og at de føler et genuint ansvar for resultatet i andre enden. Dette oppnås best gjennom *leader-leader*-modellen. Denne teorien baserer seg på at mennesket er født med *lederskap* som en grunnegenskap og ved rett anvendelse vil øke effektiviteten drastisk samt styrke hele organisasjonen (Marquet, 2012, s. xxvii).

## 2.3 Cybersikkerhet i en organisasjon – Lockheed Martin

### 2.3.1 APT – Advanced Persistent Threat

Cyber-trusler som hacking, virus og ormer kan være avanserte og vanskelige å oppdage, men få av disse truslene er designet for å angripe en spesifikk plattform. Angrep på en spesifikk plattform krever inngående kunnskap, testing og design for at angrepet skal være vellykket (Fitton, Prince, Lacy, & Germond, 2015, s. 15).

En cyber-trussel i kategorien ”Advanced Persistent Threat” er beskrevet som aktører som ønsker å angripe spesifikke mål for enten militære eller økonomiske formål. (Lockheed Martin, 2015, ss. 1-3). Særegent for APT-er viser det seg at angrepsmetodene er unike og angrepene er rettet og manuelt utført i motsetning til bruk av tradisjonelle virus som ikke angriper like spesifikt. I tillegg innehar disse aktørene høyt treningsnivå og er ressurssterke og kan drive aktive kampanjer over flere år. En APT sees på som en vanskelig og avansert trussel å hanskes med og stiller høyere krav til organisasjonens etterretningsapparat når det gjelder deteksjon av cybertrusler (Lockheed Martin, 2015).

### 2.3.2 Cyber Kill Chain-modellen

I kjølvannet av informasjonsalderens stadige utvikling mot globalisering og nettverksbasert kommunikasjon følger også aktører som for eksempel APT-er som ønsker å finne og utnytte svakheter i organisasjonene. Lockheed Martin har utviklet Cyber Kill Chain-modellen som illustrerer hvordan man kan identifisere og forhindre cyberangrep i forskjellige faser av et angrep.


**Figur 1: Cyber Kill Chain (Scalelive.com, 2016)**

Modellen kan altså benyttes for å illustrere på hvilke nivåer man bør oppdage og agere på en trussel før skadeomfanget øker. Lockheed Martin opplyser også at jo lengre ned i rekken man kommer (mot nivå 7 i figuren) jo viktigere er det å oppdage og rapportere oppover i organisasjonen; potensielt skadeomfang øker (Lockheed Martin, 2015, s. 5).

På denne måten kan modellen også brukes til å styrke cybersikkerhetskonseptet i en organisasjon. Ved å systematisk drøfte nivåene kan man identifisere svakheter, sårbarheter og angrepsveier for eventuelle fiendtlige aktører og videre arbeide for å forbedre sikkerhetskonsept og fjerne sikkerhetshull (Lockheed Martin, 2015, s. 5)

### 2.3.3 Intelligence Driven Defense

Intelligence Driven Defense er et forsvarskonsept Lockheed Martin har utviklet i forbindelse med cybersikkerhet som beskriver hvordan en organisasjon må bruke relevante erfaringer fra tidligere cyberangrep samt egen etterretning aktivt i den hensikt å oppdage og kontre cyberangrep før de skjer (Lockheed Martin, 2015, s. 4). Konseptet baserer seg på at organisasjoner som trues av APT-aktører aktivt må samle etterretning og gjøre forebyggende arbeid på egne systemer mot framtidige trusler. Her kommer også Cyber Kill Chain-modellen inn i bildet som et verktøy i å forebygge og forhindre angrep. Hensikten er å oppnå en organisasjon der etterretning fører til at angrep blir oppdaget og nøytralisert før skade er påført eller viktig informasjon blir kompromittert (Lockheed Martin, 2015, s. 3).

## 2.4 Operasjonelle konsekvenser

Fra et militært ståsted er vi avhengig av systemene ombord for å kunne planlegge og utføre maritime operasjoner. Kvartermester Kristian Wråli gjennomførte i 2017 en undersøkelse i forbindelse med sin bacheloroppgave ved FIH som tok for seg hva de operasjonelle konsekvensene ved maritime cyberangrep kan være. Problemstillingen hans var: E*r det mulig å gjennomføre cyberangrep mot navigasjonssystemet på et marinefartøy og hva ville de operasjonelle konsekvensene ved eventuelle angrep på dette systemet være?* Store deler av oppgaven til Wråli er gradert og kan derfor ikke gjengis i vår oppgave. Deler av konklusjonen hans er likevel ugradert. Her trekker Wråli frem at konsekvensene av et vellykket cyberangrep kan være svært kostbare og i verste fall føre til tap av menneskeliv. Han trekker fram at en måte å redusere risikoen for slike cyberangrep på vil kunne være å øke operatørenes kunnskap om cybersikkerhet; dette gjerne gjennom utdanningen ved Sjøkrigsskolen der det per dags dato ikke er en del av pensum (Wråli, 2017).

## 2.5 Kvasi-eksperimentet

Et kvasi-eksperiment er en form for en feltundersøkelse som er utført i et miljø hvor det er umulig å kontrollere alle variabler og innvirkende faktorer. Dette medfører at svært mange eksperiment og undersøkelser vil kunne havne under denne kategorien. Gjennom laboratorieeksperimenter kan man aktivt kontrollere alle variabler slik at man kan studere det man ønsker uten forstyrrende faktorer. Ved undersøkelser i den virkelige verden derimot, vil det sjeldent være mulig å kontrollere alle forhold som påvirker undersøkelsesobjektet (Cook & Campbell, 1979, s. 1). Det er i hovedsak problemstillingen rundt kausalitet man er ute etter å belyse. Der det i laboratorieforsøket er enklere å vise hva som forårsaker en endring, er det i feltundersøkelser mye vanskeligere å bestemme kausalitet.

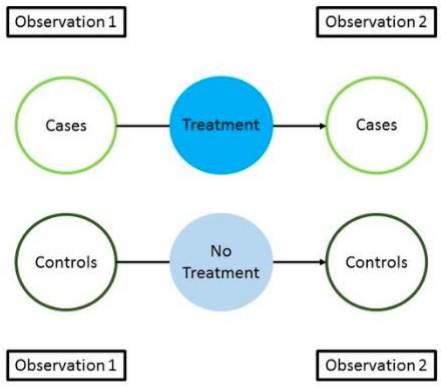
Et av hovedproblemene med alle kvasi-undersøkelser er spørsmål om validitet. Her anvender Cook & Campbell de engelske ordene *validity* og *invalidity.* Fra nå vil vi anvende *gyldighet* og *ugyldighet* i stedet. Disse begrepene brukes om det som ligger nærmest eller fjernest fra sannheten. Siden vi aldri med sikkerhet kan si hva som er årsaken til en hendelse, må vi i stedet snakke om det som er den mest sannsynlige årsaken. Dette medfører at begrepet *gyldighet* alltid innebærer en viss unøyaktighet (Cook & Campbell, 1979, s. 37). Det vil videre redegjøres for hva gyldighet innebærer i kapittel 3.

# 3 Metode

Eksperimenter innebærer ofte en test eller et forsøk av et kjent fenomen. Tester og forsøk kan gjøres i et laboratorium der man kan kontrollere alle variabler, men den virkelige verden er kaotisk og uforutsigbar. Kvasi-eksperimenter tar for seg forsøksgrupper som er forskjellig fra hverandre på andre måter enn at de i tillegg blir utsatt for ulik behandling (Cook & Campbell 1979, 6). Med andre ord, man forsøker å observere effekten av en behandling ved hjelp av to forskningsgrupper selv om gruppene ikke er identiske i utgangspunktet. For å oppfylle oppgavens hovedmål har vi valgt å utføre et kvasi-eksperiment på et utvalg kadetter ved Sjøkrigsskolen.

## 3.1 Design

Dette kvasi-eksperimentet har til formål å studere et enkelt utvalg kadetter ved Sjøkrigsskolen. Eksperimentet skal teste i hvilken grad tilstedeværelsen av en enkel operasjonsprosedyre påvirker en gruppe kadetters handlemåte i planleggingen og utførelsen av en navigasjonsøvelse med fokus på maritim cybersikkerhet. Følgende figur beskriver undersøkelsesdesignet i overordnede trekk:




**Figur 2: Non-Equivalent Control Group Design**

Undersøkelsesdesignet baserer seg på at vi til å begynne med gjør en observasjon av normaltilstanden i handlingsmønsteret til begge gruppene. Man tildeler deretter en eksperimentgruppe en behandling, for eksempel en prosedyre, mens en kontrollgruppe holdes upåvirket. Til slutt observerer vi gruppene og sammenligner handlingsmønsteret fra første til andre observasjon i den hensikt å identifisere om behandlingen har hatt noen effekt. Her er også sentrale spørsmål om gyldighet viktig å ha et forhold til.

Gjennom eksperimentet ønsker vi å observere hvordan kadettene ved Sjøkrigsskolen bruker disker (les: minnepinner) og hvordan flyten av disker mellom ulike datamaskiner foregår. I en planleggingsfase til en navigasjonsøvelse er de operative kadettene innom ulike stasjoner og datamaskiner før de til slutt utfører øvelsen på skolefartøyene eller i Navsim. Øvelsens navigasjonsruter planlegges på datamaskiner med ECDIS-programvare, såkalte planleggingsstasjoner i Navlab eller Teksim. Deretter blir rutene forflyttet med en disk fra planleggingsstasjonene til skolefartøyets eller simulatorens kartmaskin. Gjennom hele planleggingsprosessen anvender altså kadettene disker til overføring av data og rutefiler mellom forskjellige datamaskiner.

### 3.1.1 Grunnleggende antakelser

Med bakgrunn i teorien rundt maritim cybersikkerhet er det vesentlig å gjøre følgede antakelser om bruken av disker.

1. Vi går ut ifra at en tilkobling med disk til ugradert maskinvare utgjør en risiko for å infisere disken med skadevare/virus.
2. Vi går ut ifra at enhver tilkobling med disk til en datamaskin i skolefartøy/Navsim med en uscannet disk er i stand til å overføre skadevare til fartøyet/simulatorens datasystem.
3. Antivirus-PC i kontrollrom på Navkomp scanner diskene og godkjenner/underkjenner slik at de kan brukes uten risiko for spredning av skadevare på skolefartøy eller i simulator.

Med andre ord, i forbindelse med eksperimentet ser vi på all bruk av uscannede disker på datamaskiner som har med fartøyets/simulatorens systemer å gjøre som kompromitterende.

Primært ønsker vi å studere hvordan innføringen av en prosedyre som krever at disker scannes på designert antivirus-maskin før bruk på fartøy eller i simulator eventuelt endrer kadettenes handlingsmønster.

## 3.2 Innsamling av data

For å kunne observere når og hvor disker tilkobles må man kunne logge all aktivitet med disker på de aktuelle datamaskinene som er i bruk. I alt gjelder dette:

4. 6x datamaskiner på Navlab
5. 6x datamaskiner på Teksim

6. 1x datamaskin i Navsim-kontrollrom med antivirus-programvare.

Alle Windows-operativsystemer logger allerede denne aktiviteten automatisk i forbindelse med installasjon av drivere til forskjellige typer disker. Dette er ytterligere redegjort for i Vedlegg A. Dette betyr at informasjon for relativt lange tidsperioder er tilgjengelige i systemet, men utfordringen er å kunne hente ut og fremvise informasjonen på en oversiktlig måte. Dette kan imidlertid gjøres relativt enkelt med fritt tilgjengelig og gratis programvare (på engelsk: freeware) som kan lastes ned fra internett.

### 3.2.1 Frafall

Under innsamling av data regner vi med en viss mengde frafall. Grunnet størrelsen på gruppen respondenter (22 stk.) ønsker vi fortsatt en svarprosent på minst 80%. Dette for å oppnå størst mulig både ekstern og intern gyldighet i forsøket. Me andre ord ønsker vi å ha fullverdige tall på minst 18 kandidater.

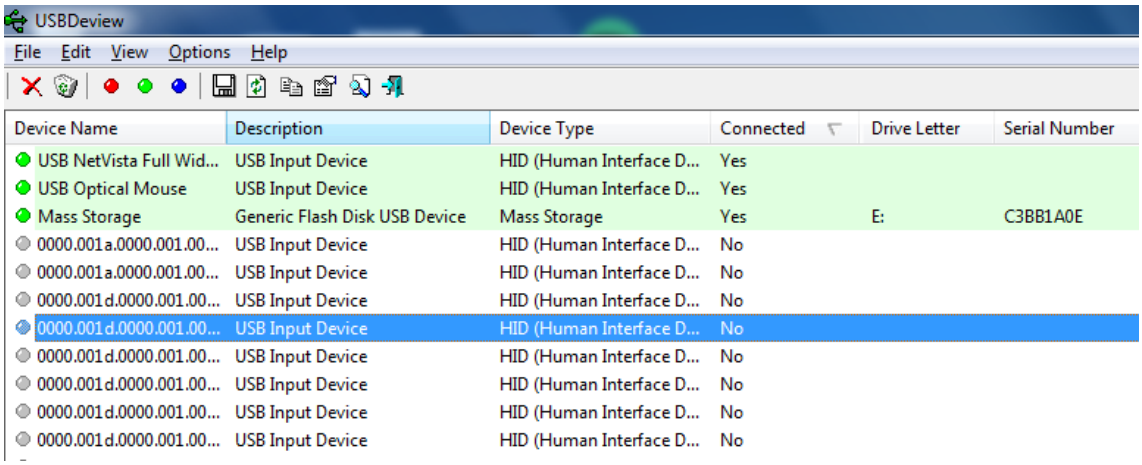
Ved et større frafall enn 20% vil vi også kunne få et anonymitetsproblem. Dette er videre drøftet i kapittel 3.3.2.

### 3.2.2 Programvare

To ulike typer programvare er benyttet i innhentingen av logg-informasjon fra de aktuelle datamaskinene. Programvarene har ulike funksjoner og brukergrensesnitt, men felles for begge to er at de viser hva som er tilkoblet datamaskinens USB-porter i sanntid samt historikk i en oversiktlig liste. De to programvarene er som følger:

**USBDeview:**

- Utgiver: NirSoft
- Gir informasjon om:
  - Serienummer på disk
  - Tidspunkt for første tilkobling av disk

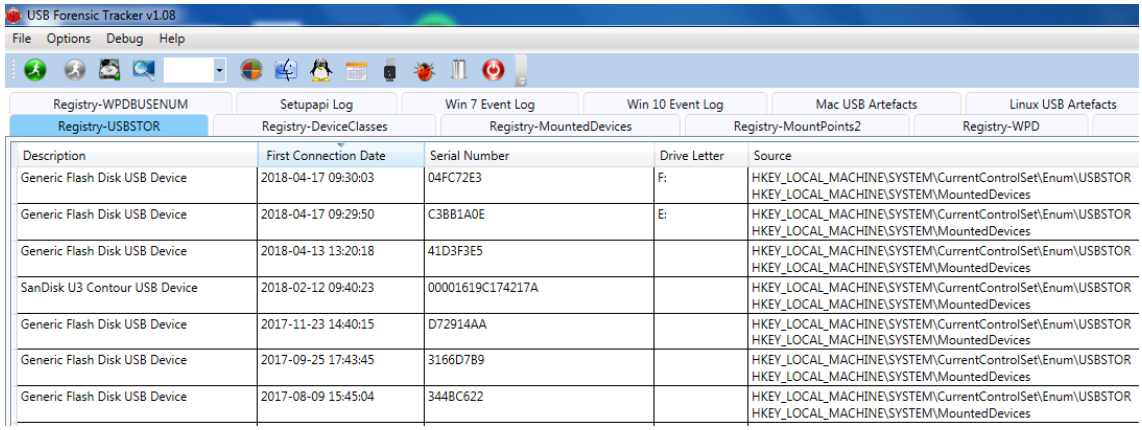



**Figur 3: Brukergrensesnitt USBDeview**

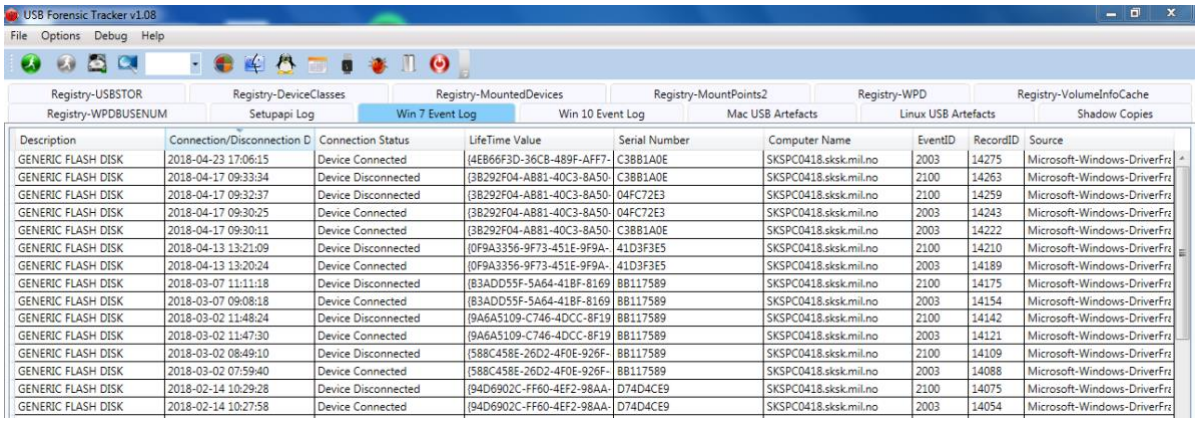
Brukergrensesnittet er enkelt og oversiktlig og denne programvaren er benyttet hovedsakelig til å registrere serienummer på diskene.

## USB Forensic Tracker:

- Utgiver: Orion Forensics
- Gir informasjon om:
  - Serienummer på disk
  - Tidspunkt for første/siste tilkobling av disk
  - Event-log: Alle tidspunkter disken er tilkoblet.
- Setter opp informasjonen i excel-dokument automatisk.




**Figur 4: Brukergrensesnitt USB Forensic Tracker**




**Figur 5: Event Log**

USB Forensic Tracker gir oss muligheten til å se på en ”event log” som viser serienummer og tidspunkt for alle tilkoblinger med USB-basert maskinvare langt tilbake i tid. Her kan også loggen «registry-USBSTOR» studeres, hvor vi får presentert samtlige serienummer som har vært tilknyttet maskinen siden installasjon av operativsystemet. Dette kan gi svært relevante data som kan benyttes i drøftingen. Grunnet forskjellene i brukergrensesnitt har det derfor vist seg å være gunstig å benytte begge programvarene i uthentingen og analysen av datasett. Bruken av to forskjellige, uavhengige programvarer gir oss også muligheten til å kryssjekke og kontrollere integriteten til informasjonen som programvarene gir oss.

## 3.3 Utvalg

Det er etablert at utvalgene i eksperimentet ikke deler de samme egenskapene og trekkene, noe som gjør at selve tolkningen av data heller blir en tolkning av hva som er forårsaket av behandlingen og hva som er rene forskjeller på utvalgene (Cook & Campbell, 1979, s. 6).

Eksperimentet utføres på kadetter ved linjen Operativ Marine ved Sjøkrigsskolen. Kadettene gjennomfører sitt andre år ved Sjøkrigsskolen og klassen teller 22 kadetter der samtlige er menn i alderen 20-30 år.

Utvalget ble delt i to like store grupper på elleve kadetter hver. Den ene gruppen fungerer som kontrollgruppe mens den andre gruppen fungerer som eksperimentgruppe. Utvalget er i tillegg delt i seilingsgrupper innad på henholdsvis tre og fire personer. Med kandidatnummer ser utvalget slik ut:

| **Kontrollgruppe** | | **Eksperimentgruppe** | |
|---|---|---|---|
| Kandidatnr. | Seilingsgruppe | Kandidatnr. | Seilingsgruppe |
| 1 | F | **12** | C |
| 2 | F | **13** | C |
| 3 | F | **14** | C |
| 4 | E | **15** | B |
| 5 | E | **16** | B |
| 6 | E | **17** | B |
| 7 | E | **18** | B |
| 8 | D | **19** | A |
| 9 | D | **20** | A |
| 10 | D | **21** | A |
| 11 | D | **22** | A |

**Tabell 1: Inndeling og kandidatnummer**

### 3.3.1 Grunnlag for utvalg

Det er flere grunner til at kadettene ved OM 2 ble valgt som forsøksgruppe. Med tanke på handlingsmønsteret rundt maritim cybersikkerhet kan det argumenteres for at en klasse midt i utdanningen passer godt til å studere hvordan holdninger og handlingsmønster ser ut. I tillegg gjennomfører OM 2 i midten av mars Øvelse Ryfylke, en navigasjonsøvelse med fokus på navigasjon i radarkontroll-mode. Dette innebærer en planleggingsfase som ender i en deployering ut på øvelsen. Det betyr at aktiviteten ved Navkomps planleggingsfasiliteter faktisk tilsvarer en planleggingsfase til navigasjonsøvelse og at dataene som kan hentes ut i ettertid har integritet. Hele klassen vil i tillegg gå gjennom samme planleggingsløp og dette sikrer en viss gyldighet i resultatene. Vi får i tilstrekkelig grad studert hvordan kadettene bruker disker mellom datamaskiner i en planleggingsfase.

### 3.3.2 Anonymitet

I forbindelse med analysen av datasettene er serienummer på disken til hver enkelt kadett registrert med tilknytning til et kandidatnummer. Gjennom analysen er serienummer registrert separat fra kadettenes navn. En svakhet vil være at serienumrene

er satt sammen i de respektive seilingsgruppene kadettene øver med. Dette medfører at det foreligger en liten sjanse for at deltakerne i undersøkelsen har en mulighet til å spørre seg frem til hvem som er hvem innad (Jacobsen, 2010, s. 50). For å motvirke dette er seilasgrupper gitt et kandidatnummer i tillegg. Det er på den andre siden ulikt antall personer innad i noen av seilasgruppene. Det vil si at det kan være mulig å gjette seg videre til hvilken seilasgruppe som har hvilket sett med serienummer.
Grunnet den antatte lave sensitiviteten i informasjonen som er samlet inn på kandidatene er vi tilfredse med anonymiteten dette gir (Jacobsen, 2010, s. 47). I tillegg vurderes det dithen at for å tolke resultatene rett er vi nødt til å presentere resultatene på en slik måte. Dette for at undersøkelsens resultater skal kunne legges frem best og minst tvetydig og for best å illustrere våre funn. Ved å bruke seilasgrupper i drøftingen åpner dette også for muligheten til å identifisere trender knyttet til seilasgruppene.
For å ytterligere sikre anonymiteten ønsker vi en svarprosent på minst 80%. Dette fordi et frafall på mer enn 20% vil bety at vi mangler tall på mer enn 4 kandidater. Det vil da bli en for stor gruppe som kan elimineres fra svarene i oppgaven, og enkeltpersoner kan da for enkelt identifiseres.

## 3.4 Behandling

For å kunne iaktta handlingsmønsteret og undersøke om konkrete retningslinjer vil endre handlingsmønsteret i nevneverdig grad, vil eksperimentgruppen motta en behandling i form av en standard operasjonsprosedyre. Eventuell observert forskjell kan likevel være forårsaket av forhold vi ikke er klar over i utgangspunktet. Det er derfor viktig at vi som forskere systematisk evaluerer egen metode og analyserer forhold og faktorer som kan gi endring i kadettenes handlemåte selv uten behandling (Cook & Campbell, 1979, ss. 38, 55).

I forbindelse med eksperimentstart ble eksperimentgruppen tildelt prosedyren i gjennom en felles brief for utvalget. Prosedyren er utformet med hensikt å sikre at disker blir scannet med antivirus-programvare på en bestemt datamaskin i Navsim-kontrollrom før de benyttes på skolefartøy eller i Navsim. Prosedyren er gjengitt i sin helhet i Vedlegg B. Eksperimentgruppen ble instruert å ikke opplyse resten av klassen om prosedyren. Ettersom data og serienummer var mulig å registrere og hente ut i ettertid, ble ikke kontrollgruppen informert.

## 3.5 Framgangsmåte

Selve gjennomføringen er en kritisk faktor for at resultatene skal bli så robuste som mulig. Følgende framgangsmåte viser steg for steg hvordan eksperimentet skulle gjennomføres:

1. O1: Uthenting av datasett før behandling ble introdusert (26. Februar 2018)
    a. Logger ble kun hentet ut fra AV-maskin ettersom det var på denne maskinen vi ønsket å observere behandlingens effekt.
2. X: Brief og innføringen av prosedyre for eksperimentgruppen (28. Februar 2018)
    a. Øvingsordren ble utsendt 28. Februar. Dette markerer starten på planleggingsløpet til utvalget.
    b. Utreisedato for seilingsgrupper:
        i. E og F: 11. Mars = 10 planleggingsdøgn
        ii. C og D: 15. Mars = 14 planleggingsdøgn
        iii. A og B: 19. Mars = 18 planleggingsdøgn
3. O2: Uthenting av datasett etter behandling når siste seilingsgruppe hadde startet seilas (etter 19. Mars 2018).
    a. Uthenting av logger fra samtlige 13 datamaskiner (som nevnt i 3.2).

## 3.6 Styrker og svakheter

I lys av relevant teori kan det drøftes flere styrker og svakheter med selve metoden. En viktig faktor som preger metoden er undersøkelseseffekt. Gjennom metoden ønsker vi å studere virkeligheten og da ønsker man ikke å forstyrre denne i noen grad (Jacobsen, 2010, s. 30). Problemet oppstår da med nærhet mellom forsker og forskningsobjekt. I vårt tilfelle kan vi si at det er en viss nærhet mellom oss og utvalget. Personlig kjenner vi de fleste gjennom vennskapelige relasjoner, noe som kan gi en viss grad av undersøkelseseffekt. På den andre siden er dette en faktor man aldri helt kommer uten fordi at det alltid vil forekomme en viss form for undersøkelseseffekt (Jacobsen, 2010, s. 30).

Vi kan også komme utfor et problem Cook & Campbell beskriver som *local history*. I et forsøk er det stor sjanse for at andre faktorer i omgivelsene påvirker forsøksgruppene i tillegg til behandlingen (Cook & Campbell, 1979, ss. 105-106). I denne sammenhengen kan vi se på tidsrommet som en slik faktor. Den ene gruppen har for eksempel kortere tid på seg å planlegge enn den andre. Som nevnt i forrige kapittel innebærer

fremgangsmåten en viss forskjell i utreisedato. Fra første til siste gruppe går det 8 dager, dvs. at den ene gruppen har 8 døgn lenger tid på å planlegge. Dette kan gi påvirkning på resultatene og være en svakhet for metoden.
På mange måter representerer utvalget en av de største variablene i vår metode. Utvalget består av 22 enkeltindivider som hver for seg opptrår og oppfører seg svært forskjellig. Svakheten ligger i å trekke resultater og slutninger rundt handlemønsteret til kadettene når vi ikke har klart for oss hva som påvirker dem. En eksakt sannhet er umulig å framstille. På den andre siden er det flere trekk ved metoden som tar vekk betydelige feilkilder. Vi vet at utvalget skal gjennom det samme planleggings- og seilingsløpet. Dette gjør altså at utvalget har en felles oppgave de skal løse på relativt lik måte. Det kan da bli mer plausibelt å trekke slutninger basert på forskjellene i handlemønsteret. Likevel vil det være en sannsynlighet for årsaken til endring i handlemønster ikke er som følge av behandlingen. Det vil altså være usikkerhet rundt kausaliteten.
Det kan være visse feilkilder knyttet til håndteringen av dataprogrammer. Selv om programmene er testet og gir tilsynelatende riktige resultater, er det knyttet en viss usikkerhet til det som fremvises. På den andre siden er det en styrke faglig sett å med stor grad av enkelhet kunne observere bruken av disker på et så omfattende nettverk av datamaskiner. Enkelheten gjør det svært effektivt å samle inn data til analyse. Det er i tillegg en styrke at vi benytter to forskjellige og uavhengige programvarer i den hensikt å kryssjekke funksjonaliteten og at programvaren virker.

## 3.7 Gyldighet og reliabilitet

Gyldighet omhandler i hvilken grad resultatene etter undersøkelser viser sannheten i den virkelige verden. Gyldighet innebefatter også i hvilken grad man kan fastslå kausaliteten i en hendelse. Vi kan skille mellom begrepsgyldighet, intern gyldighet og ekstern gyldighet (Jacobsen, 2010, s. 19). Andre forfattere skiller derimot kun mellom intern og ekstern gyldighet (Cook & Campbell, 1979). Vi ønsker kun å benytte begrepene intern gyldighet, ekstern gyldighet og reliabilitet i denne oppgaven.

### 3.7.1 Intern gyldighet

Spørsmålet om intern gyldighet oppstår når man skal bestemme kausalitet når to variabler kovarierer, samt hvilken retning kausaliteten fungerer (Cook & Campbell, 1979, s. 50). Eksempelvis: er det A som fører til B eller omvendt, eller finnes det en

annen variabel C som fører til B? Intern gyldighet kan også omhandle hvorvidt vi har dekning i våre data for de konklusjonene vi trekker (Jacobsen, 2010, s. 19).
I henhold til fremgangsmåten beskrevet i kapittel 3.5 har vi innført en behandling hos eksperimentgruppen i form av en prosedyre. Når det kommer til intern gyldighet blir det da essensielt å drøfte resultatene etter behandlingen på grunnlag av at det kan være andre faktorer som fører til endret atferd i utvalget.
Vi ønsker å redegjøre for de mest relevante formene for trusler mot intern validitet.
Over tid kan problemet rundt *modning* (på engelsk: Maturation) oppstå. En observert endring eller effekt kan komme som et resultat av at respondenter i utvalget modnes, blir mer erfaren, smartere osv. i tiden mellom Observasjon 1 og Observasjon 2. Det blir da vanskeligere å peke hva som egentlig forårsaker endringen (Cook & Campbell, 1979, s. 52).
En annen trussel er *instrumentering* (på engelsk: Instrumentation). En observert effekt kan være forårsaket av instrument/måleenhet man bruker i O1 og O2. Dette dreier seg også om at menneskene som bruker måleinstrumentene blir mer erfaren med utstyret i løpet av forsøksperioden (Cook & Campbell, 1979, s. 52). Et eksempel for vår del vil være bruken av programvare som innsamlingsverktøy, noe som drøftes ytterligere i kapittel 4 og 5.
Når to forskjellige grupper mottar en behandling oppstår trusselen rundt *seleksjon* (på engelsk: Selection). En observert effekt kan skyldes forskjeller innad gruppen og ikke nødvendigvis som følge av behandlingen som gis (Cook & Campbell, 1979, s. 53).
Tvetydighet (på engelsk: Ambiguity) omkring kausalitet kan også påvirke intern gyldighet. Denne trusselen oppstår når tredjeparts-variabler utelukkes og det blir uklart om f.eks. A forårsaker B eller B forårsaker A. Usikkerhet oppstår da omkring hva som forårsaker hva (Cook & Campbell, 1979, s. 53)
Estimering av intern validitet er en nøysom prosess som krever at forsøkspersonell hele tiden systematisk gjennomgår og vurderer innsamlet data. Når det er gjort kan en begynne å eliminere faktorer i den hensikt å konkludere med graden av kausalitet i forsøket (Cook & Campbell, 1979, s. 55)

### 3.7.2 Ekstern gyldighet

Ekstern gyldighet omhandler hvorvidt resultater og funn i en studie er gyldige i andre sammenhenger og utvalg (Jacobsen, 2010, s. 20). Det er også forskjell på hvorvidt et resultat kan generaliseres. For eksempel vil det være forskjell på om et resultat kan

generaliseres for andre målgrupper og om et resultat kan generaliseres på tvers av populasjoner (Cook & Campbell, 1979, s. 71). I vårt tilfelle vil det eksempelvis være interessant å drøfte i hvilken grad funnene våre i OM 2 kan gjelde for kommende OM-klasser eller kadetter generelt ved Sjøkrigsskolen.

Det finnes flere ulike trusler mot ekstern gyldighet. *Utvalg og behandling* (på engelsk: Selection and treatment) innebærer at sammensetning av utvalg og hvordan deltakelse i forsøket avvikles er avgjørende for om resultatet kan generaliseres. Eksempelvis bør man gjøre deltakelsen så beleilig som mulig for respondentene. Et eksperiment som kun tar 10 minutter å gjennomføre kan i mye større grad være mulig å generalisere enn et forsøk som f.eks tar en hel dag (Cook & Campbell, 1979, s. 73).

I forbindelse med målpopulasjoner har vi trusselen rundt *situasjon og behandling* (på engelsk: Setting and treatment). Hvorvidt er det mulig å generalisere årsaken til en effekt på tvers av organisasjoner/bedrifter som for eksempel fabrikker, byråer, militærleirer osv. Frivillighet er her en viktig faktor; frivillige organisasjoner har høyere motivasjon for å delta i undersøkelser og det påvirker generaliserbarheten (Cook & Campbell, 1979, s. 74).

Det finnes som oftest en viss målgruppe man ønsker å kunne generalisere forsøksresultater for. Det er derfor viktig at forsøksgruppen har en viss representativitet i forhold til målgruppen (Cook & Campbell, 1979, s. 74).

### 3.7.3 Reliabilitet

Reliabilitet omtaler integriteten i metodikken og gjennomførelsen av eksperimentet, med andre ord, om eksperimentet er til å stole på. Store målefeil og uriktige resultater setter ned reliabiliteten (Jacobsen, 2010, s. 20).

Reliabilitet bestemmes av forskerens nøyaktighet i utforming og gjennomføring av forsøket. Målinger med lav reliabilitet kan påvirke og forsterke feil og gi uriktige resultater hos eksperimentgruppen. For å øke reliabilitet lønner det seg blant annet å teste grupper i stedet for enkeltindivider (Cook & Campbell, 1979, s. 43). Her kan også valget om åpen eller skjult observasjon spille inn; det antas at reliabiliteten blir bedre hvis et utvalg observeres fra det skjulte. Denne observatøreffekten vil kunne skape spesielle resultater (Jacobsen, 2010, ss. 160, 167).

Måten behandling blir implementert på er også en kilde til enten god eller dårlig reliabilitet. For eksempel vil det være en viss forskjell når ulike personer innfører

samme behandling. Denne mangelen på standardisert behandling vil nedsette sjansen for å oppnå sanne resultater (Cook & Campbell, 1979, s. 43).
Som nevnt i kapittel 3.7.2 er det mange forhold som tilsier om et resultat kan generaliseres eller ikke. Graden av reliabilitet (i samspill med graden av intern gyldighet) vil påvirke forutsetningene for hvorvidt konklusjonene kan generaliseres (Jacobsen, 2010, s. 371).

# 4 Resultat

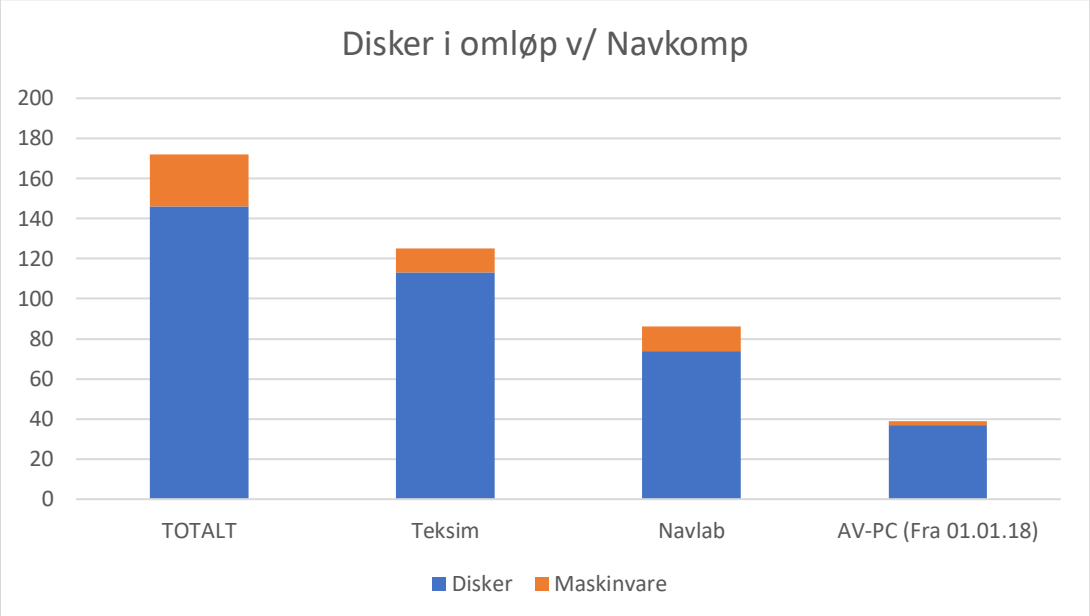
Dette kapitlet tar for seg resultatene etter kvasi-eksperimentet. Som beskrevet i kapittel 3.5 er fremgangsmåten delt i 3 hoveddeler: Observasjon 1 (pretest), Behandling X og Observasjon 2 (posttest). Vi ønsker å presentere resultatene i kronologisk rekkefølge samt analysere hva funnene egentlig sier.

## 4.1 Observasjon 1

Observasjon 1 (heretter referert til som O1) fungerte på mange måter som en pretest av hvordan tilstanden ved bruken av antivirus-scanning fungerte til vanlig. Vi var her i stand til å hente ut data helt tilbake fra 2017, men valgte å avgrense oss til 1. Januar 2018. Dette grunnet brukertekniske problemer med antivirus-datamaskin som gjorde at vi ikke hadde pålitelige data fra før 2018. Dette redegjøres for senere.

### 4.1.1 Disker i omløp v/ Navkomp

Datainnsamlingen ble gjort med godkjenning fra Navkomp uten at noen i utvalget ble gjort oppmerksom på dette. Dette kan derfor sees på som en skjult observasjon og dermed er utvalgets handlinger i svært liten grad påvirket av observasjonen.
Tabellen under viser spesifikt hvor mange disker som er i omløp ved de forskjellige stasjonene på Navkomp gjennom de enkelte datamaskinenes respektive levetid.



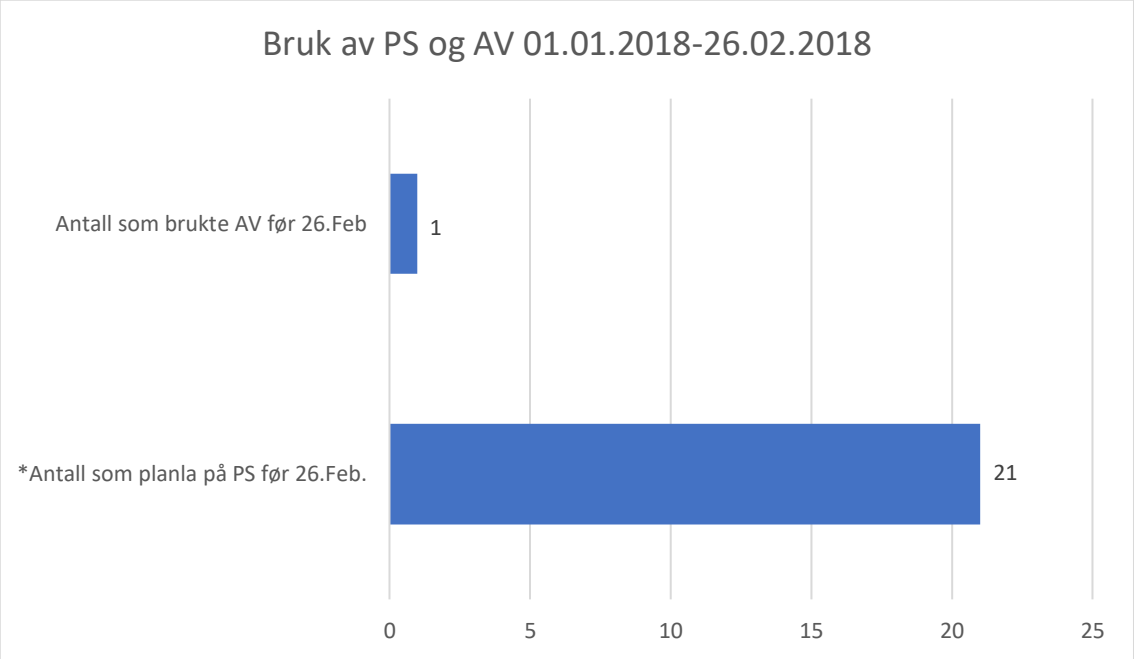

**Tabell 2: Disker i omløp før behandling**

Overordnet er det om lag 172 unike serienumre på forskjellig typer maskinvare i omløp, på Teksim siden desember 2016 og Navlab siden september 2017. På Teksim er det

identifisert 125 ulike serienummer mens det på Navlab er identifisert 86 ulike serienummer. På antivirus-datamaskinen (heretter omtalt som AV-maskinen) er det identifisert rundt 40 ulike serienummer fra 01.01.2018. Dette viser altså at disker brukes på tvers av Navlab og Teksim. Mange av disse serienumrene tilhører maskinvare som mus og tastatur og det er da nærliggende å tro at ca. to serienummer per datamaskin tilhører mus og tastatur. Visuell granskning av datasettene har i stor grad bekreftet denne hypotesen. Med 6 maskiner i Teksim, 6 maskiner i NavLab og 1 antivirus-maskin i Navsim-kontrollrom får vi da ca. 26 serienummer som ikke er lagringsenheter. Vi kan derfor estimere at opp til 146 forskjellige lagringsenheter har vært brukt i NavKomps datamaskiner, datert tilbake til henholdsvis 2016 i Teksim og september 2017 for Navlab. Det er altså et betydelig antall mennesker og personlige lagringsenheter knyttet til bruken av disse datamaskinene.

### 4.1.2 Handlingsmønster og brukerfeil

Neste tabell viser spesifikt utvalgets handlingsmønster før prosedyren ble innført hos eksperimentgruppen. Denne er vesentlig for å bestemme om en eventuell behandling har hatt en effekt.




**Tabell 3: Aktivitet ved PS- og AV-maskiner før behandling**

*Tall om bruk av PS før 26.02.18 delvis hentet fra samtaler med kandidatene.

Av dataene ser vi at kun én kandidat har vært innom AV-maskinen før prosedyren ble innført. For videre tolkning av disse resultatene er det relevant å redegjøre for en brukerfeil av programvaren som ble identifisert i etterkant av eksperimentet.

Brukerfeilen omhandlet hovedsakelig at vi manglet forståelse for hvordan de forskjellige loggene produsert av programvaren ble lagret. Spesielt to forskjellige typer logger skulle benyttes for å bestemme kandidatenes aktivitet. Vi skulle benytte en logg som viste siste tilkoblingstidspunkt med en disk samt en ”event log”, en hendelsesloggføring, som ga info om alle til- og frakoblinger til maskinen. Sistnevnte logg oppdaget vi at sletter seg selv etter hvert som nye disker tilkobles. Kombinert med at vi kun samlet inn informasjon fra AV-maskinen den 26. Februar 2016, gjør dette at vi ikke kan fastslå gjennom data alene om kandidatene aktivt benyttet sin disk i planlegging til navigasjonsøvelser. Dette utgjør en stor trussel mot reliabiliteten til eksperimentet, ettersom det da ikke kan fastsettes gjennom datasettene hva som er O1, altså handlemønsteret før behandlingen innføres. Denne informasjonen må derfor erstattes med annet datagrunnlag.

For å få data å jobbe med for denne perioden kontaktet vi to kandidater og utspurte dem om klassens seilingsaktivitet. I O1-tidsperioden hadde utvalget gjennomført en kveldsseilas med tilhørende planleggingsperiode. Kandidatene kunne bekrefte at alle utenom én kadett hadde planlagt og gjennomført denne navigasjonsøvelsen. Dette medfører at vi fortsatt har bakgrunn for å si noe om hvordan kandidatene gjennomførte planleggingsprosesser før prosedyren ble innført, men dette kan ikke vises direkte gjennom elektroniske spor. De muntlige kildene anser vi for å være svært pålitelige. Dette, samt de faglige kravene om at alle kadetter individuelt skal planlegge og gjennomføre seilas gjør det rimelig å anta at planlegging ville foregå på lik måte ved senere øvelser, som for eksempel Øvelse Ryfylke, dog i en annen skala.

I forbindelse med forberedelser til navigasjonsøvelser har hver kadett tilgang på en egen disk utgitt av skolen for overføring av filer. Etter oppklarende samtaler med ulike respondenter i utvalget kom det fram at de fleste benytter sin disk, men at noen seilingsgrupper deler en felles disk innad av logistiske årsaker. Ut ifra denne informasjonen, samt antakelsen gjort i forrige avsnitt, kan vi anta at de fleste seilingsgruppene til vanlig benytter en form for disk i planleggingsløpet sitt, men at

individene selv ikke nødvendigvis legger igjen elektroniske spor med egen disk. Vi kan derfor jobbe videre med antakelsen om at det er mulig at et treff på AV-maskin innad i en seilingsgruppe kan indikere at disker scannes på vegne av hele seilingsgruppen før bruk på skolefartøy. Vi kan også anta at selv om ikke individer i utvalget ser ut til å bruke sine disker, er vedkommende likevel i noen grad aktiv med seilingsgruppens disk og dette kan derfor gi indikasjoner på kandidatens handlemønster når det gjelder datasikkerhet.

### 4.1.3 Oppsummering O1

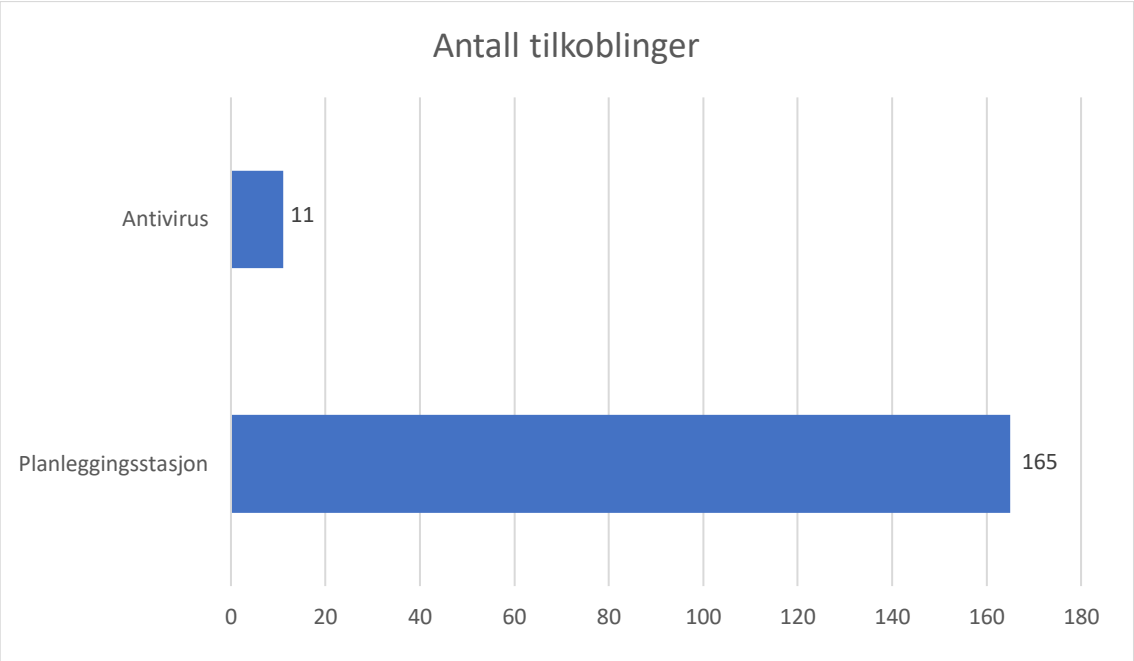
Vi ser gjennom O1, i sammenheng med antagelsene, at 21 av 22 kandidatene er innom en planleggingsmaskin i forbindelse med en navigasjonsøvelse. Dette er et normalt handlemønster. Vi ser videre at én av 21 har anvendt AV-maskinen i noen som helst form. Ser vi på antagelsen om at en seilingsgruppe benytter en felles disk, anser vi 3 (antall kandidater i den aktuelle seilingsgruppen) for å være det høyeste antall kandidater som hypotetisk sett kan ha benyttet scanning av disk med en eller annen hensikt. Med andre ord er det en sjanse for at opptil 3 kandidater kan ha anvendt AV-maskinen gjennom den ene tilkoblingen. Ut ifra resultatet er det likevel tydelig at bruken av AV-maskin på ingen måte er utbredt i utvalget før en prosedyre innføres.

## 4.2 Observasjon 2

Observasjon 2 (heretter referert til som O2) ble foretatt 22.03.2018 i etterkant av Øvelse Ryfylke i form av en datainnsamling fra samtlige datamaskiner på Teksim, Navlab i tillegg til AV-maskinen i Navsim-kontrollrom. Datagrunnlaget for O2 strekker seg fra 26. Februar – 22. Mars 2018. Eksperimentgruppen i utvalget ble informert om prosedyren 28. Februar 2018.

### 4.2.1 Aktiviteten på Navkomp

I perioden mellom utgivelse av prosedyre og eksperimentslutt ser vi at det er registrert et stort antall tilkoblinger ved datamaskinene på Navkomp.




**Tabell 4: Aktivitet etter behandling**

Diagrammet viser antall tilkoblinger gjort av forsøksgruppen totalt sett fra slutten av februar til 22. mars. Ut ifra dette er det tydelig at det er høy aktivitet ved maskinene i den aktuelle perioden. Av datasettet kommer det også frem at disker brukes hyppig på forskjellige maskiner. Med andre ord dukker samme disk opp både i Navlab og Teksim med hyppig mellomrom.

Grunnet brukerfeilen nevnt i forrige delkapittel er ikke dataene fra planleggingsstasjonene fullstendig. Mens noen logger fyller perioden fra 26.02.2018 til 22.03.2018, viser andre mer trafikkerte datamaskiner kun data fra tidlig mars (eksempelvis 8. eller 10. mars) noe som gjør selve antallet feil. Likevel sier dette oss at det i løpet av en planleggingsperiode er minst 165 tilkoblinger totalt på planleggingsstasjonene. Basert på gjennomsnittlig antall tilkoblinger per dag kan vi estimere opptil 250 tilkoblinger på maskinene gjennom det aktuelle tidsrommet. Dette står i stor kontrast til antallet tilkoblinger til AV-maskinen hvor vi ser at aktiviteten er langt mindre. For å se om prosedyren følges korrekt må vi derfor se nærmere på siste tilkoblingstidspunkt før avreise.

### 4.2.2 Siste tidspunkt for tilkobling

I forbindelse med prosedyren er det relevant å se på siste tilkoblingsdata i en planleggingsstasjon og se dette opp imot siste tilkobling i en AV-maskin. Dette er presentert i tabellen under:

| Kand. nr. | Sist i TS/NL | Sist i AV | Utreisedato | Seilings-gruppe |
|---|---|---|---|---|
| 1 | 10.03.2018 13:05 | 10.03.2018 12:47 | | F |
| 2 | 10.03.2018 16:26 | - | | F |
| 3 | 10.03.2018 13:05 | - | | F |
| 4 | N/A | N/A | **11.03.2018** | E |
| 5 | 09.03.2018 22:09 | - | | E |
| 6 | N/A | N/A | | E |
| 7 | 09.03.2018 19:36 | - | | E |
| 8 | 13.03.2018 07:58 | - | | D |
| 9 | 14.03.2018 14:50 | - | | D |
| 10 | 13.03.2018 14:32 | - | | D |
| 11 | 14.03.2018 12:26 | - | **15.03.2018** | D |
| 12 | 14.03.2018 12:09 | 09.03.2018 10:32 | | C |
| 13 | 13.03.2018 12:35 | - | | C |
| 14 | 07.03.2018 12:20 | 14.03.2018 11:25 | | C |
| 15 | N/A | N/A | | B |
| 16 | 17.03.2018 19:33 | - | | B |
| 17 | 14.03.2018 12:40 | - | | B |
| 18 | - | - | **19.03.2018** | B |
| 19 | 18.03.2018 16:32 | 09.03.2018 11:36 | | A |
| 20 | 18.03.2018 17:45 | - | | A |
| 21 | 15.03.2018 15:11 | 15.03.2018 17:05 | | A |
| 22 | 18.03.2018 17:42 | - | | A |

| Eksperimentgruppe | N/A | AV etter Teksim/Navlab (Iht. Prosedyre) |
|---|---|---|

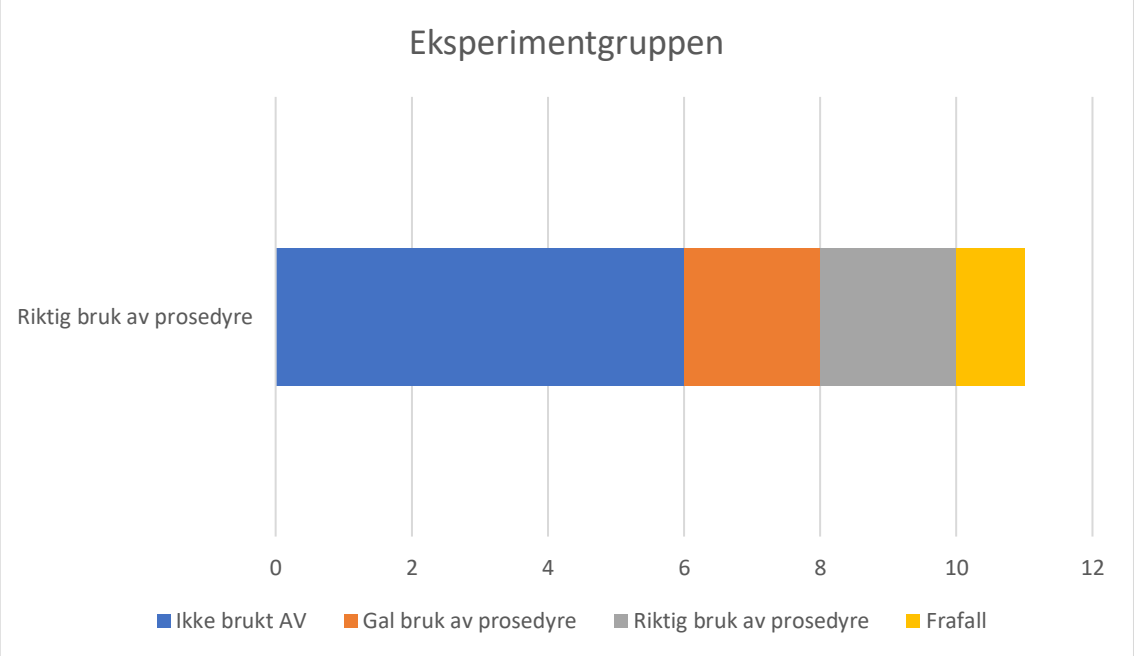
**Tabell 5: Siste tilkoblingstidspunkter**

Overordnet ser vi at de fleste disker er i bruk i de aktuelle tidsrommene. Dette indikerer at egen disk blir benyttet selv om seilingsgruppen har felles disk innad, som går mot antakelsen om felles disk.
Av 22 individer i forsøksgruppen har 3 stykker forlagt sin disk og vi har derfor ikke data på disse kandidatnumrene. Kandidatnummer 18 har ikke brukt sin disk i løpet av perioden, men blir likevel presentert her.

### 4.2.3 Eksperimentgruppen

I eksperimentgruppen er det tilsynelatende kun 2 kandidater som har anvendt prosedyren rett slik vi hadde tiltenkt den å fungere, hvorav én av disse også benyttet AV-maskin i O1 (kandidat 14). Av de resterende har 2 scannet diskene sine på et tidspunkt, men vært innom en planleggingsmaskin i ettertid. Etter antakelsen om at planleggingsmaskinen potensielt kan infiseres medfører dette kompromittering av disken. I praksis indikerer dette at disse 2 reiser ut på fartøyet med disker som ved bruk vil kunne skade fartøyets systemer.

Fem kandidater (seks totalt markert blått, hvorav én har ikke anvendt disk i det hele tatt) har anvendt sin disk i planleggingsstasjonene i Navlab/Teksim, men ikke anvendt AV-maskin.



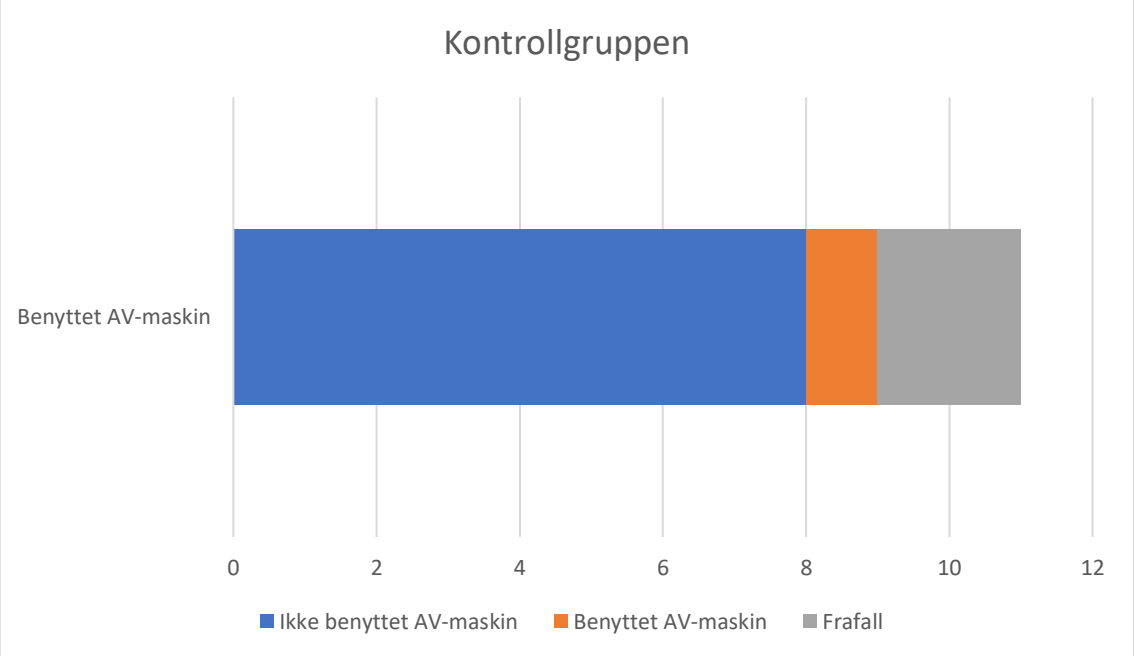

**Tabell 6: Aktivitet i eksperimentgruppen**

Resultatene gir oss to forskjellige teorier på hva handlemønsteret kan være. Den første går ut på at hvis seilingsgruppene benytter en felles disk og den kandidaten som har

gjennomført scanning i henhold til prosedyren er den som har alle rutene på sin disk, betyr det at 2 av 3 seilingsgrupper har gjennomført prosedyren etter vår intensjon. Den andre teorien sier mer eller mindre det motsatte. Ved nærmere analyse av tilkoblingsdatoene i tabell 5 ser vi at av de to kandidatene som har fulgt prosedyren slik den var tilsiktet, har kandidat 21 i seilingsgruppe A en tidligere *sist tilkoblet*-dato enn de resterende kandidatene i gruppen. Dette betyr at de resterende kandidatene har vært innom en planleggingsmaskin med sin egen disk etter siste gang den antatte "hoveddisken" i gruppen har vært tilkoblet. Tatt i betraktning at planleggingsmaskinene kun anvendes til planlegging av ruter til navigasjonsøvelser, kan dette antyde at kandidatene har planlagt ruter på PS etter siste tilkoblingsdato for den antatte hoveddisken. Dette tilsier at prosedyren ikke er gjennomført korrekt for gruppen totalt sett, men kun for de enkeltstående diskene. Den andre teorien går dermed ut på at vi ikke konsekvent kan drøfte med en felles disk innad gruppene, men derimot må se på alle diskene som individuelle.

### 4.2.4 Kontrollgruppen

I kontrollgruppen har én kandidat anvendt AV-maskinen i planleggingsperioden, men ikke utført scanning i henhold til prosedyren. Med frafall på to personer grunnet forlagt disk, betyr dette at 8 kandidater i kontrollgruppen ikke har benyttet AV-maskin på noen måte i tidsrommet 26.02.18-22.03.18.

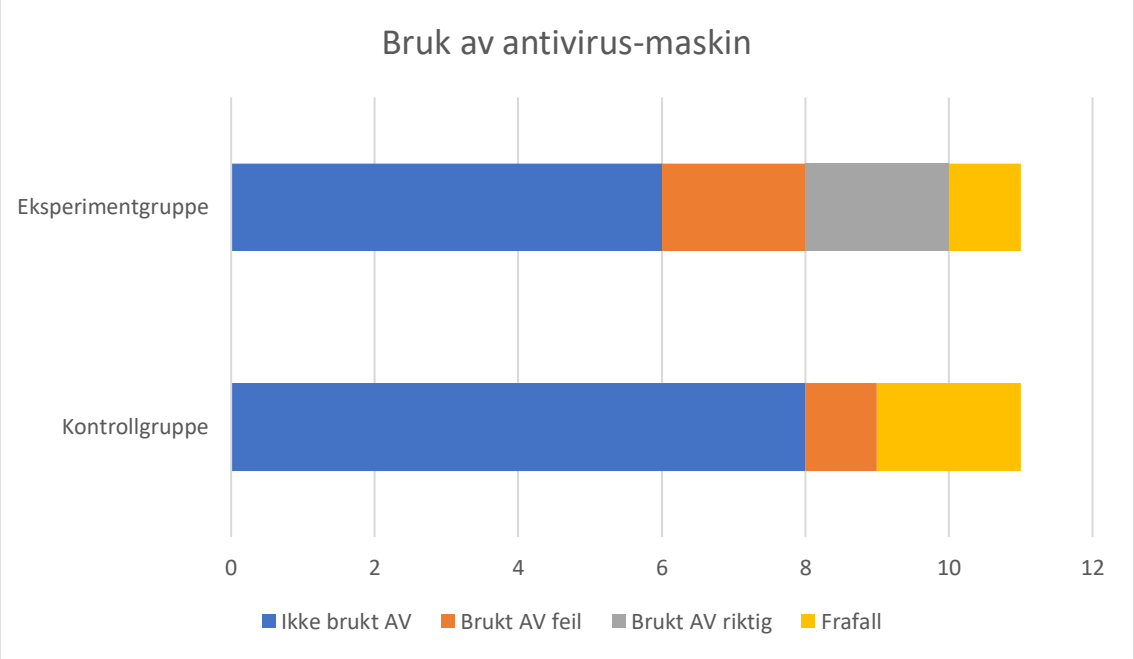



**Tabell 7: Aktivitet i kontrollgruppen**

Fra O1 til O2 ser vi at det er en økning på 1 kandidat, fra 0 til 1, som anvender AV-maskinen i det hele tatt, men ikke i henhold til prosedyren.

### 4.2.5 Sammenligning

Vi ser ut ifra resultatene at kandidater i eksperimentgruppen har benyttet prosedyren og utført scanning av disker i henhold til kravene etter at prosedyren er utgitt i konkret form. Kontrollgruppens handlemønster bærer i stor grad de samme trekkene som utvalget hadde ved O1. Det er likevel fremdeles en stor bestanddel av enkeltindivider i eksperimentgruppen som ikke benytter AV-maskinen til tross for at prosedyren er innført.




**Tabell 8: Sammenligning av handlingsmønster**

### 4.2.6 Oppsummering O2

Fra O1 til O2 ser vi at kontrollgruppen har en endring i handlemønster ved én kandidat. Her ser vi en endring fra ingen tilkoblinger til én tilkobling i AV-maskinen.
I eksperimentgruppen ser vi en endring fra én til fire tilkoblede disker fra O1 til O2. Hvis vi anvender teorien om at kandidatene benytter én disk per seilingsgruppe vil dette kunne bety at vi i O2 kan ha opp mot fire i kontrollgruppen og åtte i eksperimentgruppen som har endret handlemønster. Likevel, grunnet tidsintervall mellom planlegging, scanning og utreise kan det se ut som at dette ikke stemmer og at

seilingsgruppene samlet sett ikke har fulgt prosedyren i henhold til teorien. Vi kan derfor konkludere med at aktiviteten må betraktes individuelt og at vi ser en atferdsendring hos flere kandidater i eksperimentgruppen, men at prosedyren i liten grad er utført på riktig måte.

## 4.3 Andre faktorer

Under analysen av resultatene har vi avdekket enkelte andre faktorer enn vår innførte behandling som kan ha hatt en innvirkning på resultatene.

### 4.3.1 Eksisterende prosedyre

En vesentlig faktor som kan påvirke utvalget er tilstedeværelsen av en allerede gjeldende prosedyre. Etter samtale med ledelsen i NavSim ble det informert muntlig om at en prosedyre for bruk av AV-maskinen eksisterer, noe vi som kadetter og har hørt snakk om til tider. Det fremkommer derimot ikke en skriftlig prosedyre som er allmenn kjent eller offisiell SOP. Det fremstår som at enkelte med teknisk ansvar og kompetanse i Navsim mener det foreligger en prosedyre for bruk av disker i simulatorlokalene, men at denne prosedyren ikke har blitt like godt formidlet som det tilsynelatende har vært inntrykk av blant teknisk personell på Navkomp. Samtaler med kadetter antyder at denne prosedyren ikke eksisterer og vitner til at det kan eksistere forskjellige holdninger til bruk av disker i NavSim.

### 4.3.2 Innføring av eksperimentprosedyren

Etter O1 ble det igangsatt en behandling av eksperimentgruppen. Dette bestod av innsamling av serienummer på diskene til alle kandidatene i denne gruppen og gjennomgang av prosedyren vi ønsket at de skulle bruke. De fleste fikk denne gjennomgangen med den ene av oss, mens et fåtall resterende fikk gjennomgangen av den andre på et senere tidspunkt av forskjellige grunner. I første omgang var kun den ene av oss til stede, noe som medførte at den andre ikke fikk med seg nøyaktig hvordan dette ble gjort. Gjennomgangen for de andre kandidatene ble derfor ikke gjennomført nøyaktig likt den første runden. Et poeng med innføringen av prosedyren var at kandidatene i minst mulig grad skulle skjønne at de var del av et eksperiment. Det ble derfor lagt vekt på at prosedyren ikke kom fra oss, men var en ny offisiell prosedyre fra Navkomp som skulle følges.

# 5 Drøfting

I dette kapittelet ønsker vi å bryte ned funnene etter eksperimentet og se hvilke sammenhenger som kan bekreftes eller avkreftes mellom kandidatenes atferd og innføringen av prosedyren. I tillegg er det interessant å se på hva den observerte handlemåten kan føre til når det gjelder tenkte trusler mot maritim datasikkerhet.

Drøftingen vil bli presentert i 4 delkapitler der vi går gjennom eksperimentets ulike bestanddeler. I første omgang er det relevant å diskutere frafallet av data og hvordan dette kan påvirke resultatene. Videre ønsker vi å se nærmere på O1 når det gjelder hvilke handlingsmønstre som allerede eksisterer i utvalget. For å kunne si noe om prosedyrens effekt og påvirkningskraft ser vi deretter på O2 og utforsker hvordan prosedyren fungerer og hvilke handlemønstre som oppstår hos eksperimentgruppen. Opp imot temaet maritim cybersikkerhet er det relevant å trekke linjer mellom det observerte handlemønsteret og ulike trusler.

## 5.1 Frafall

I ethvert forsøk vil det være frafall i form av kandidater som enten ikke responderer eller det ikke finnes data på. Disse kandidatene kan ikke regnes som respondenter og vil ikke bidra til resultatet, men årsaken og omfanget av frafallet må tas i betraktning. Frafallet i eksperimentet vårt er vanskelig å diskutere på grunn av måten eksperimentet er gjennomført på. Data har blitt hentet inn på samtlige kadetter med en lagringsenhet i forkant, for å så spørre om tillatelse til å anvende dataene til forskning etterpå. Dette gjør at det eksisterer kun en mindre mulighet for frafall som følge av en bevisst handling hos kandidaten. Dette åpner muligheten for at vi som forskere direkte påvirker frafallsprosenten i den hensikt å påvirke kandidatenes handlingsmønster så lite som mulig. Fordelen med dette er opplagt; man ønsker å unngå undersøkelseseffekten hos utvalget. Likevel kan det føre til at frivilligheten hos utvalget ”endres” i den forstand at kandidater som eventuelt ville reservert seg fra å delta i undersøkelsen lar vær å gjøre dette. På den måten kan selve undersøkelsesprosessen ha påvirket frafallet. Det er en fordel for oss som forskere, men kan være problematisk fra et etisk perspektiv.

I kontrollgruppen mangler vi tall på 2 kandidater grunnet mangel på egne disker. I eksperimentgruppen mangler vi tall på 1 av samme årsak.

I kapittel 3 ble det presisert at vi trengte 80% deltakelse fra respondentene for å anse reliabiliteten til undersøkelsen til å være innenfor det vi anser for å være godt nok. Med et frafall på 3 av 22 kandidater sitter vi igjen med en svarprosent på 86,36%. Dette er over 80% og derfor tilstrekkelig.

Som nevnt tidligere forekommer det at seilingsgruppene ofte benytter én hoveddisk innad. Flere kandidater har oppgitt at de avslutter planleggingsperioden med at alle rutefilene som skal brukes på skolefartøyene samles på én disk. Dette for å forenkle prosessen med å sammenføye ruter til én samt begrense antall forskjellige ruter som legges inn for å forhindre forvekslinger. En konsekvens av dette er at hvis en kandidat ikke anvender sin disk, vil vedkommende fortsatt kunne planlegge som vanlig. Ved endt planlegging velger kandidaten i stedet å låne disken som er blitt designert til å samle alle rutene på innad i sin egen seilingsgruppe. Dette kan gi et frafall av ukjent størrelse og i tillegg påvirke datasettene vi har uthentet. En kandidat vil altså kunne gjennomføre en plan- og øvelsesprosess uten å legge igjen elektroniske spor. Denne typen frafall vil med andre ord ikke nødvendigvis si at kandidaten ikke har vært gjennom de samme prosessene som sine kollegaer, men at prosessen er gjennomført med en disk som ikke er registrert på han selv. Det er derfor en sannsynlighet for at denne problemstillingen kan gjelde alle de 3 kandidater som er identifisert uten disk, men også hvilken som helst annen kandidat.

Vi anser respondentdeltakelsen for å være innenfor fastsatt svarkrav. Det er ikke nevneverdig størrelsesforskjell på frafallet i gruppene. Dette øker gyldigheten i sammenligningsgrunnlaget.
Antallet kandidater som ikke lenger har en disk og som derfor må anvende en annen kandidats disk er svært lavt. Disse telles som frafall i datasettene, men det har blitt bekreftet gjennom samtaler med kandidatene at disse fortsatt planlegger som vanlig og anvender en lånt disk som antatt. Grunnet det lave antallet dette gjelder anses dette ikke å senke reliabiliteten eller gyldigheten i eksperimentet.

## 5.2 Observasjon 1

I denne del drøftes funnene rundt O1. Med fokus på målene for oppgaven totalt sett er det i denne del viktig å finne et så godt bilde som mulig på hva som er virkeligheten når

det gjelder bruken av disker ved Navkomps maskiner. Vi er altså ute etter å finne årsakene til hvorfor kandidatenes handlemønster er som det er. For å oppnå dette må vi ta for oss viktige antakelser[1] som legges til grunn for drøfting, samt hva resultatene etter datainnsamling faktisk kan bety.

### 5.2.1 Mangel på data

Resultatene viser fra O1 at svært få av kandidatene til vanlig anvendte AV-maskin i forbindelse med ruteplanlegging. Som nevnt førte brukerfeilen fra vår side til at kandidatenes aktivitet på PS ikke ble logget elektronisk, men antatt gjennom samtaler og oppklaringer med et utvalg kandidater. På den ene siden er det ugunstig at vi mangler konkret data på denne aktiviteten. Hensikten med behandling og O2 er som kjent å observere om det skjer endring i atferd som følge av behandling, noe som gjør at et manglende datagrunnlag fra O1 er skadelig for eksperimentets gyldighet. Denne problemstillingen faller inn under en av truslene mot intern gyldighet: instrumentering. Vi kan altså stille spørsmål om eksperimentets interne gyldighet er god, siden mangel på data fører til usikkerhet om vi faktisk måler endring i atferd som følge av behandlingen eller ikke.

På den andre siden er antakelsene som gjøres på mange måter sterke. Vi får gjennom samtalene et konkret vitnemålsutsagn på at samtlige kandidater (med unntak av ett frafall) gjennomførte en kveldsseilas på normal måte. Det vil si at hver kandidat fikk en ordre, måtte planlegge en rute i henhold til øvingsmål og overføre denne til skolefartøy for utførelse av seilas. Vi har i tillegg gått igjennom samme løpet selv og er godt kjent med hvordan det foregår. Dette gir oss et bilde på at normaltilstanden med tanke på bruken av planleggingsstasjoner er relativt ukomplisert: ruter planlegges på maskinene og overføres deretter med disk. Når det gjelder AV-maskinen er denne dataen logget og hentet ut per 26.02.2018 og vi har dermed konkrete elektroniske data. Det vil si at det kritiske spørsmålet, ”benytter kandidatene AV-maskin før seilas til vanlig?” kan besvares ved analyse av datasettet. Dette tilsier derfor at vi har et godt grunnlag for å måle det vi ønsker å måle og at intern gyldighet er god.

Prosessen som fører til mangelfullt datagrunnlag er også i stor grad et spørsmål om reliabilitet i undersøkelsesmetoden. På mange måter er dette som følge av at vi valgte å benytte ukjent programvare til innsamling. Hvis vi hadde hatt kjennskap til hvordan

[1] Presenteres i Kap. 4.1.2

loggene fungerte, ville vi kunne samlet inn med et jevnere intervall og dermed konstruert logger som viste hele perioden. Dette ville i større grad gitt komplette data som hadde fjernet usikkerheten ved manglende data. Likevel er utfordringene rundt reliabilitet og verktøy man har liten kjennskap til høyst vanskelig å forutse og man blir tvunget til å lære og utforske verktøyene mens man jobber. Eksempelvis for vårt tilfelle kan dette gå utover resultatene, gyldigheten og eksperimentet i sin helhet og man blir tvunget til å jobbe ut ifra antakelser eller andre datagrunnlag. Hensikten er forøvrig alltid å opprettholde gyldighet til tross for lavere grad av reliabilitet slik at vi kan dra meningsfulle og sanne slutninger basert på virkeligheten.

### 5.2.2 Handlemønster

Med grunnleggende antakelser i bunn samt datagrunnlag fra AV-maskin er det nå mulig å trekke slutninger om hvilke handlemønstre kandidatene innehar uten at en konkret prosedyre er tilstede. Som nevnt i resultatkapitlet er bruken av AV-maskin svært begrenset hos utvalget i O1-perioden. I januar 2018 ble denne datamaskinen først innfaset med AV-programvare og dette kan ha ført til at de fleste ikke har fått med seg dette og derfor latt vær å bruke den. Likevel finnes det i følge teknisk personell ved Navsim en eksisterende prosedyre som sier at disker skal scannes før bruk, men denne er ikke konkretisert skriftlig og følges ikke opp av noen ved Navkomp. Det er altså opp til brukerne selv å scanne disken sin på eget initiativ, noe som kan si oss hvorfor bruken er så lite utbredt.

Kandidatene hadde i løpet av O1-perioden kun gjennomført en planleggingsprosess i forbindelse med semesterets første kveldsseilas. Med tanke på intern gyldighet er det derfor en ulempe at ikke flere planleggingsprosesser er representert i dataene. Det er problematisk å måle en tendens til bruken av AV-maskinen når datasettet kun gir oss et bilde på én enkelt planprosess. I lys av dette ville gyldigheten vært sterkere dersom dataene hadde omfattet flere prosesser over tid slik at vi kunne identifisert mer tydelige tendenser blant kandidatene. På den andre siden er det derimot O1 en valid punktobservasjon eller stikkprøve på hvordan tilstanden er med det utdanningsgrunnlag kandidatene har så langt. 21 individuelle kandidater har gjennomført prosessen som på sin side kan gi et godt bilde over eventuelle trender. Den eksisterende prosedyren sier ifølge teknisk personell Navkomp at disker skal scannes før bruk hver eneste gang de skal benyttes på Navsim og før seilas med skolefartøyene. Det skal derfor ikke finnes

unntak, noe som styrker den interne gyldigheten i O1. I tillegg blir sammenligningsgrunnlaget etter behandling mer eller mindre likt: kandidatene skal gjennom en ny planleggingsprosess til en ny øvelse og må derfor gjennomføre prosessen på lik måte. Sammenligningen mellom O1 og O2 vil drøftes nærmere senere i oppgaven.

Hvis vi skal kunne generalisere funnene i O1-perioden er det flere faktorer som kan indikere graden av ekstern gyldigheten. Det er viktig i henhold til oppgavens målsetning å diskutere hvorvidt funnene kan gjelde andre utvalg ved skolen og særlig kandidater ved samme linje. Når det gjelder trusler mot ekstern gyldighet er representativitet viktig. Utvalget vårt er selektert som offiserer på samme grunnlag og går gjennom det samme opplegget som kommende kadetter ved samme linje vil gjøre. Dette gir større grad av ekstern gyldighet. Å generalisere til et utvalg som tilsvarer andre linjer eller hele skolen og kadettmassen i ett kan derimot vise seg vanskeligere siden utdanningsløpene foregår svært forskjellig. Ingen andre enn kandidater ved Operativ Marine vil for eksempel gjennomgå navigasjonsøvelser med tilsvarende planleggingsprosesser. Siden det er denne situasjonen vårt eksperiment spesifikt undersøker vil det være mindre sannsynlig at resultatet vil generaliseres til et utvalg ved en annen linje. På den andre siden er forholdet til prosedyrer mer eller mindre en faktor som preger de fleste bransjer og grener av Forsvaret som tilsier at forskjellige utvalg muligens vil forholde seg til prosedyrer på samme måte. Ut ifra dette kan det argumenteres for at hvilken som helst kadett som utfører hvilken som helst lignende planprosess vil utsettes for de samme faktorene som vårt eksperiments kandidater og dermed vil gi lignende resultater. Kulturen for datasikkerhet på Sjøkrigsskolen er på mange måter uklar og dette kan i større eller mindre grad gjelde alle linjene ved skolen. Dette argumentet er likevel vanskelig å vekte ut ifra eksperimentets resultater alene og fører heller til spekulasjon om hvordan de forskjellige linjene utvikles gjennom utdanningsløpet. Vi kan derfor si at det er en mulighet for at funnene kan generaliseres til hele skolen.

### 5.2.3 Konklusjon

Vi anser samtalene med kandidatene for å få klarhet i deltakelsen under plan- og gjennomføringsprosessen til kveldsseilaset før 26.02.18 for med høy sannsynlighet å være gyldige. Dette fordi vi selv har nær kjennskap til hvordan dette gjennomføres samt faglige krav satt av skolen. Vi anser derfor resultatene i O1 for å være gode nok til å

kunne si noe om kandidatenes handlemønster og senere holdninger rundt omgang med disker mellom forskjellige datasystemer.
Alle utenom én kandidat har i O1 gjennomgått en plan- og gjennomføringsprosess av en navigasjonsøvelse. Dette vil si at 21 kandidater har planlagt på en planleggingsstasjon. Kun én av disse er registrert tilkoblet AV-maskinen før 26.02.18. Ut fra dette vil vi kunne påstå at det ikke er normalt handlemønster for en kandidat å scanne disken før seilas.
Når det gjelder ekstern gyldighet mener vi at funnene i stor grad kan generaliseres til kommende og eksisterende utvalg ved OM-linjen. Vi mener også at det er mulig å generalisere funnene til hele Sjøkrigsskolen med bakgrunn i de svært entydige funnene i eksperimentet. Disse slutningene tar utgangspunkt i dagens utdanningsmodell.

## 5.3 Observasjon 2

I denne del ønsker vi å drøfte og problematisere rundt funnene i O2. Først må følgende antakelser gjentas:

- Vi antar at ved enhver tilkobling til AV-maskin utføres en scanning av disken. Disken er per definisjon da vasket og "ren".
- Vi antar at utreise uten "ren" disk kan kompromittere fartøyet med skadevare.

Resultatet viser at det kun er to kandidater som har brukt prosedyren riktig i henhold til kravene satt av oss. Hvordan kan det ha seg at resterende ni kandidater i eksperimentgruppen tilsynelatende har unnlatt å scanne diskene sine til tross for en stående prosedyre?

### 5.3.1 Prosedyren

Ved innføring av en ny prosedyre vil det alltid være en mulighet for at enkelte mottakere forstår, tolker og mottar budskapet på en litt annen måte enn det som initialt var tiltenkt av sender (Dahl & Befring, 2010). Resultatet av dette blir i vårt tilfelle at det med stor sannsynlighet vil hende at noen kandidater har opptrådt på en måte som er utenfor det vi i utgangspunktet hadde sett for oss. Vi ser for eksempel at tre kandidater anvender AV-maskinen, men i feil rekkefølge i henhold til prosedyren. Dette kan skyldes en annen forståelse av hensikten med prosedyren og det kan være at noen tror at én vellykket scanning av en disk etter å ha vært tilkoblet en PS tolkes som at stasjonen er «ren» og kan behandles som dette også i ettertid. Etter å ha sett på flyten av disker mellom forskjellige PS-er vet vi at en slik tolkning vil være svært feilaktig, men likevel

mulig. Dette ser likevel ut som en misforståelse fordi informasjon om at planleggingsstasjoner kan være infisert muligens ikke er kommunisert skikkelig. I dette scenarioet er det da prosedyrens implementering, ordlyd og oppfølging som er mangelfull og fører til misforståelser og kompromittering. På den andre siden kan det også skyldes forsømmelser fra kandidatenes side, som følge av tidspress, forglemmelse eller holdning til prosedyrer. Det er likevel tydelig at muligheten er stor for ulik forståelse og oppfattelse under kommunikasjon og implementering av en prosedyre.

Prosedyren ble formidlet til kandidatene av oss som medkadetter og for å ikke gjøre det for åpenbart at de var med i undersøkelse ble det oppgitt eksplisitt at prosedyren var et nytt tiltak fra Navkomps side. Det kan derfor stilles spørsmål ved autoriteten bak budskapet og dets formidling. Kandidatene kan altså ha ilagt prosedyren mindre seriøsitet enn det som var tiltenkt fra vår side og derfor ikke ha tatt forglemmelser og forsømmelser så tungt. Det kan her stilles spørsmål ved om det kunne gitt andre resultater at instruktører ved Navkomp eller en faglærer i navigasjon hadde introdusert prosedyren for kandidatene. I dette tilfellet er det en mulighet for at kandidatene hadde behandlet prosedyren mer seriøst med bakgrunn i faktorer som bedømmelse i fagene, karakterer og helhetsinntrykk. Med andre ord kan det tenkes at kandidatene i større grad frykter konsekvenser ved neglisjering av en prosedyre fra en tydelig autoritetsperson enn de gjør fra oss som medkadetter.

Gyldigheten i spørsmålet rundt prosedyrens effekt er en vanskelig problemstilling med mange mulige innfallsvinkler. Som tidligere nevnt har kandidatene mulighet og kutyme for å anvende én felles disk innad i seilasgruppen for å samle det endelige produktet av ruteplanleggingen. Ut ifra våre resultater er det vanskelig å påvise og det kan på overflaten tolkes dithen at kandidatene som ikke har anvendt AV-maskin har neglisjert prosedyren. En mulighet kan derimot være at de har brukt en annen disk og derfor like fullt oppfylt kravene satt i prosedyren. I resultatkapitlet lanserte vi derimot teorien om at gruppene ikke benytter en felles, ren disk på grunn av at siste tilkoblingstidspunkt mellom antatt felles disk og gruppenes andre disker ikke stemmer overens med utreisetidspunkt. Med andre ord så foregår det planlegging i tiden mellom vasking av ”ren” disk og utreise. Dette åpner for muligheten at kompromitterte disker med oppdaterte ruter benyttes ombord på fartøyene, noe som utelukker at gruppen i sin helhet har fulgt prosedyren. Til videre drøfting er det altså dette som gjør det nødvendig

å se på hver disk individuelt i den hensikt å avgjøre i hvilken grad prosedyren som behandling har endret handlingsmønsteret hos kandidatene.

### 5.3.2 Endring i handlemønster

I denne del tar vi for oss drøftinger rundt endringen i kandidatenes handlemønstre. Problemstillingen rundt en korrekt gjennomført prosedyre legges ikke vekt på til fordel for selve endringen i atferd siden rekkefølgen kun er i henhold til prosedyren hos to kandidater, begge fra eksperimentgruppen.

Sett ut ifra resultatene etter O2 kan vi betrakte endringen i handlemønster fra flere forskjellige hold. Fra O1 til O2 ser vi en viss endring i handlemønster hos enkeltkandidatene i eksperimentgruppen ved at fire kandidater (kontra én fra O1) har benyttet AV-maskin under planleggingen (oppført i tabell 5). Først og fremst er det en stor mulighet for at denne atferdsendringen skyldes den korte tiden mellom innføringen av prosedyren og starten på planleggingsperioden og seilas. Det foreligger derimot også en god mulighet for at andre faktorer kan ha spilt inn. Enkelte kandidater kan ha hatt kjennskap til prosedyren som Navkomps ansatte muntlig har formidlet fra tid til annen. Resultatene fra O1 kan tyde på dette ettersom én kandidat har anvendt AV-maskinen før 26.02.18, med antakelsen om at virusscan ble gjennomført. En annen årsak kan være at enkelte kandidater har et forhold til datasikkerhet av egen interesse og derfor velger å scanne disken av personlige årsaker. Slike årsaker kan variere stort i mangfold og utforming og kan påvirke utvalget i større eller mindre grad. Kandidatene kan i tillegg påvirke andre rundt seg, men det er vanskelig å måle ut ifra elektroniske spor. Det er derfor en stor utfordring å vurdere relevansen til så lite målbare parametre, men det er viktig å ta de i betraktning. Disse faktorene kan også knyttes til gyldighetspørsmålet som vil bli problematisert senere i kapitlet.

Fra O1 til O2 ser vi med andre ord at kontrollgruppen går fra å ha ingen som anvender AV-maskinen til å ha én. Dette er et vanskelig resultat å forholde seg til fordi det tilsynelatende ikke finnes noen synlig årsak til avviket. Dette kan derimot være med på å bekrefte tilstedeværelsen av de usikre faktorene nevnt i forrige avsnitt. Slike faktorer kan derfor ha en større innvirkning på utvalget enn det vi i utgangspunktet trodde og må derfor regnes med når vi skal konkludere med hva som gir atferdsendring. På den andre siden er endringen likevel størst hos eksperimentgruppen, noe som tilsier at innføringen av den mer håndfaste prosedyren likevel kan ha hatt størst påvirkningskraft.

Etter behandlingen har altså fire nye kandidater anvendt AV-maskin, hvorav én tilhører kontrollgruppen. Dette antyder altså at det foreligger andre faktorer som motiverer kandidatene til å scanne disken.

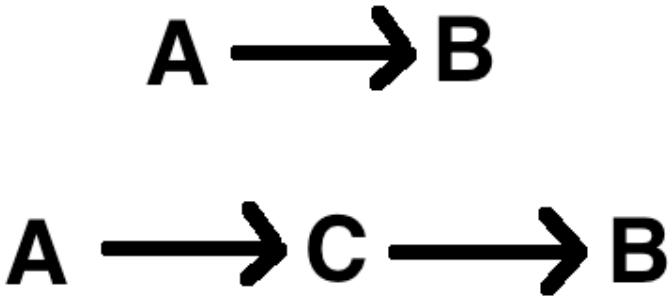
Om fokuset rettes mot seilingsgruppene er endringen som følge av behandlingen langt større. Her må vi benytte teorien om at seilingsgruppene benytter en felles disk som er ”ren” ved utreise. Da viser resultatene at 2 av 3 seilingsgrupper i eksperimentgruppen har én kandidat hver som har fulgt prosedyren på en korrekt måte. Med andre ord kan vi anta at opptil syv kandidater i eksperimentgruppen har fulgt prosedyren eller vært med i en gruppeprosess der prosedyren er fulgt opp. I kontrollgruppen kan vi på likt grunnlag anta at én seilingsgruppen á 3 kandidater kan ha et forhold til AV-scan, men her ble likevel ikke prosedyren fulgt på en korrekt måte. Dette er likevel en problematisk tilnærming grunnet datagrunnlagets integritet. Tidligere i oppgaven er det nevnt at det ved samtale med kandidatene er kommet fram at noen grupper benytter en felles disk. Det finnes ingen konkrete garantier på at alle gruppene gjør det samt om dette fører til at en ”ren” ukompromitterbar disk benyttes på seilas. Disse faktorene senker derfor gyldigheten rundt å betrakte resultatet med fokus på seilingsgrupper i stedet for enkeltkandidater.

### 5.3.3 Sammenligning

I denne del drøftes selve sammenligningen av O1 og O2, hvordan resultatene kan tolkes og integriteten i resultatet. Som nevnt i kapittel 5.2.1 førte en brukerfeil i forbindelse med innsamlingen av data til at en sammenligning mellom O1 og O2 kunne bli ugyldig. Gjennom andre undesøkelsesmetoder ble likevel O1 vurdert som gyldig sammenligningsgrunnlag for O2.

Som kjent fra forrige delkapittel var det mulig å observere en tydelig atferdsendring fra O1 til O2. Atferden endret seg ikke bare i eksperimentgruppen, men også i kontrollgruppen til tross for minimal påvirkning. Hvis vi ser bort ifra prosedyren kan det endrede handlemønsteret skyldes flere faktorer. Som nevnt tidligere kan egen holdning til datasikkerhet eller kjennskap til eksisterende prosedyre spille inn. Andre faktorer kan omfatte undervisningsopplegget samt utviklingen kandidatene gjennomgikk i faget sitt mens eksperimentet pågikk. Dette vil dermed bli en trussel mot intern gyldighet i kategorien modning. Kandidatenens tilegning av kunnskap og utviklig

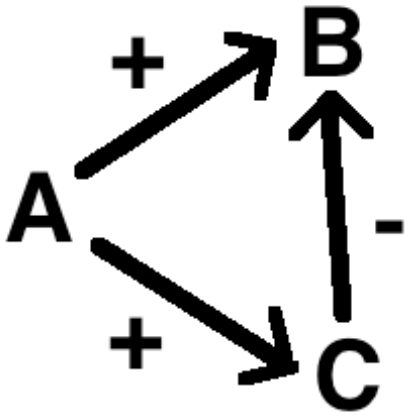
gjennom planprosessen over tid kan ha vært med å påvirke i hvilken grad de tok høyde for datasikkerhetstrusselen.




**Figur 6: Tvetydighet innen intern gyldighet I**

Figur 5.1 (Cook & Campbell, 1979, s. 50) kan gi et enkelt bilde på hvordan et forhold mellom kjente og ukjente variabler kan se ut. Figuren viser en situasjon hvor man innfører behandling A og observerer endring B. Ut ifra dette resultatet ser det tilsynelatende ut som at A resulterer i B, mens det i virkeligheten må tas høyde for at det er en tredje faktor C som egentlig fører til B. Det blir da svært viktig å ta i betraktning alle tolkninger rundt eventuelle tredjepartsvariabler når vi vurderer årsak og effekt (Cook & Campbell, 1979, s. 50). Kandidatenes undervisningssituasjon kan være et eksempel på dette. Undervisning innen navigasjonssystemer og datatrusler kan sammen med innføring av vår behandling i samme tidsrom gi kandidatene forsterkede inngangsverdier og forståelse for datasikkerhet som eksempelvis fører til at de i større grad begynner å anvende AV-maskin i planlegging. I denne situasjonen vil det ikke være et direkte A → B-forhold, men et mer sammensatt bilde med tilstedeværelse av tredjepartsfaktorer. Det blir derfor vanskelig å finne den konkrete årsaken til effekten, i dette tilfelle atferdsendring.

Innføringen av prosedyren, undervisning, endret handlingsmønster hos kandidatene samt andre ukjente faktorer kan korrelere uten at faktorene nødvendigvis er tilknyttet hverandre. Vi må derfor se på det store bildet og hva som egentlig kan ha størst effekt på utvalget og i tillegg drøfte hvordan faktorer kan påvirke hverandre.




**Figur 7: Tvetydighet innen intern gyldighet II**

Figuren over beskriver hvordan ulike faktorer kan påvirke hverandre. En økning i A vil her gi en økning i C og B (gitt ved + tegn), men en økning i C vil gi en reduksjon i B (Cook & Campbell, 1979, s. 50). Dette kan i vårt tilfelle gjelde på flere forskjellige måter. Ut ifra resultatene har kun fire av elleve personer i eksperimentgruppen (der to kandidater frafalt) blitt registrert på AV-maskin i løpet av O2-perioden. Gjennom figuren over kan vi for eksempel se på A som prosedyren, C som total arbeidsmengde og B som graden av opprettholdt datasikkerhet. Å følge en prosedyre parallelt med alle andre aktiviteter som foregår under et planleggingsløp er enda en ekstra arbeidsoppgave. Vi kan derfor ikke utelukke at innførelsen av prosedyren har økt arbeidsmengden hos kandidatene og dermed kan ha ført til forsømmelse og redusert bruk av prosedyren. Med andre ord kan innførelsen av en prosedyre på en slik måte vi gjennomførte det ha fungert mot sin hensikt.

Det er likevel andre forhold som tilsier at til tross for økt arbeidsmengde, burde ikke dette gi utslag i seilingsgruppene. Oppgaven er relativt enkel: prosedyren krever at rene disker benyttes på fartøyene. Hvorfor viser ikke gruppene i større grad tegn til å reise ut med rene disker? Hvorfor er graden av forsømmelse så stor? Dette kan muligens forklares ved å se nærmere på X: den tekniske innføringen av prosedyren. I denne sammenhengen kan man dra inn *leder-følger*-forholdet: idéen om at man kan dele menneskegrupper i ledere og følgere der lederne skal sørge for å styre tanker, planer og handlinger hos undergitte (Marquet, 2012, s. XXV). I vårt tilfelle kan denne teorien overføres: lav grad av ansvarliggjøring kan ligge til grunn for manglende individuell

oppfølging av prosedyren. Arbeidet i dagens organisasjoner krever mer av menneskers kognitive evner. Når overordnende behandler sine undergitte som følgere, kan dette føre til lavere motivasjon hos undergitte til å gjøre sitt beste (Marquet, 2012, s. XXVI). På den ene siden kan det tenkes at motivasjonen for å følge en prosedyre helst bør komme innenfra. Det optimale er at kandidatene selv føler viktigheten og ansvar for å opprettholde datasikkerheten i organisasjonen. Forsømmelsen vi observerer gjennom resultatene kan derfor komme som følge av dette. Manglende intensjon, ansvarliggjøring og forståelse for hvorfor prosedyren eksisterer og må benyttes kan ha gitt de påfølgende resultatene. Dette åpner for at det kan være et lederskapsspørsmål hvorvidt en prosedyre vil fungere effektivt eller ikke.

### 5.3.4 Konklusjon

Sammenligningen av O1 og O2 gjort med bakgrunn i en del antakelser vi anser for å bære stor grad av gyldighet, men disse gir også noe usikkerhet. Vi ser ut fra O2 at behandlingen gir en viss observerbar effekt. Fra å ha kun én bruker av AV-maskinen i O1 har vi fem i O2. Av disse fem er én i kontrollgruppen og fire i eksperimentgruppen. To av de sistnevnte har gjennomført prosedyren slik den var tiltenkt. Vi har gjennom delkapitlet diskutert muligheten for at kandidatene har anvendt én felles disk innad seilingsgruppen og at dette derfor kan bety at to av gruppene i eksperimentgruppen har utført prosedyren slik den var tiltenkt. Dette kan avkreftes gjennom granskning av tilkoblingstidspunkt og utreisedato.

Resultatene viser en merkbar endring, men det er vanskelig å se spesifikke årsaker til hvorfor endringen er som den er. Det kan derfor være et større antall tredjepartsfaktorer i spill. Vi har i denne sammenhengen sett på økt arbeidsmengde, utestående ansvarliggjøring og manglende forståelse for hvorfor prosedyren skulle gjennomføres som de mest relevante faktorene. Vi kan derfor konkludere med at vi ikke vet helt sikkert hvorfor prosedyren ikke har gitt ønsket effekt i større grad enn det som var observert.

## 5.4 Nivået av maritim cybersikkerhet

Gjennom dette kapitlet ønsker vi å se resultatene fra eksperimentet i sammenheng med relevant teori knyttet opp mot maritim cybersikkerhet. Vi vil med andre ord se på hvilken kultur for datasikkerhet som eksisterer på Navkomp når det gjelder utdanning av kadetter. Vi ønsker å se på utfordringer rundt tiltak og potensielle sikkerhetshull samt hvilke konsekvenser dette kan medføre.

### 5.4.1 Utfordringer

Som vi har sett gjennom eksperimentets resultater kan det være store utfordringer knyttet til innføring av en ny sikkerhetsrutine som for eksempel en prosedyre. Relevant teori sier blant annet at spesifikk utdanning av personell som skal anvende teknologien er et konkret tiltak som bedrer datasikkerheten (Wråli, 2017). Det ble også drøftet i kapittel 5.3.3 at ansvarliggjøring av den enkelte kadett kan være et tiltak som kan øke fokuset på datasikkerhet fordi det kan det kan motvirke mekanismer som fører til forsømmelse av tillagte arbeidsoppgaver. Forståelse for hvorfor en oppgave utføres er altså essensielt for at personellet skal utføre oppgaven godt (Marquet, 2012). I kombinasjon med bedre utdanning på området kan det derfor være viktig at brukerne av systemene skjønner farene ved å håndtere datasystemer med viktig informasjon (uansett gradering) og samtidig selv føler ansvar for at denne informasjonen bør håndteres best mulig. Dette kan likevel bli en vanskelig prosess ettersom man trenger etablerte miljøer for å drive god opplæring av andre. Det kan fort bli en ønskedrøm at kadetter skal videreføre og opprettholde kulturen selv uten oppfølging fra lærere og veiledere. Det kan videre argumenteres for at slik oppfølging og kompetente miljøer innen datasikkerhet krever for mye tid og ressurser å utvikle og man kan stille seg spørsmålet: Er det verdt det? Er det viktig at kadettene ved Sjøkrigsskolen blir dyktige og bevisste på datasikkerhetstrusler? Dette blir da en debatt om bestilling fra Sjøforsvaret og strategi fra skoleledelsens side. Med andre ord, en problemstilling som kan være svært vanskelig for kadetter å påvirke. I dette spørsmålet blir datagrunnlaget vårt fra eksperimentet alene for tynt. Eksperimentet sier sitt om fraværet av rutiner og vanskeligheten av innføring av nye rutiner, men det foreligger et betydelig antall gyldighetstrusler som gjør det viktig å supplere med annen forskning. Vi kan derfor si at en eventuell strategiendring bør basere seg på ytterlige forsøk og undersøkelser. På skolen er det i hovedsak lærere og stabsansatte som lærer bort sine kunnskaper og holdninger til kadettene. I lys av dette mener vi at en undersøkelse eller intervjuserie av

stabsansatte, med fokus på Navkomp-personell i operativ sammenheng, vil kunne bidra til å kartlegge behovet for et opplæringsregime og eventuelle holdningsendringer i lærerstaben. De ansatte representerer kontinuiteten i utdanningen fra år til år og deres kunnskaper, ferdigheter og holdninger kan derfor være roten til god opplæring hos kadettene.

### 5.4.2 Tiltak

Hvis vi ser bort ifra strategi og det overordnede bildet kan vi fokusere og drøfte rundt tiltak på det nivået vi har studert fram til nå, kadettene. For å innføre en prosedyre eller et tiltak som fungerer tilfredsstillende antas det at ansvarliggjøring av kompetente brukere vil være en mer effektiv tilnærming. På Sjøkrigsskolen er det per i dag ingen eller få[2] kurs eller opplæring som dreier seg spesifikt rundt dette; det er altså et fravær av denne type utdanning. Konkrete tiltak som bør gjøres vedrørende utdanningen på Sjøkrigsskolen, spesifikt ved linjen Operativ Marine, kan være å legge inn kurs, fagemner og opplæring om datasikkerhet så tidlig som mulig. Dette fordi vi kan se gjennom eksperimentets forskjellige faser at det finnes tendenser hos kadettene der man unnlater å følge prosedyrer. Det er også gjennom samtaler med Navkomps ansatte og kandidatene klart at en prosedyre kanskje eksisterer, men at denne ikke er kommunisert eksplisitt nok. Opplæring kan for eksempel inneholde eksempler på trusler og angrep som har blitt gjennomført tidligere og referere til funn i oppgaver og undersøkelser i den hensikt å vise hvilke muligheter og farer som cyberangrep medfører. Organisasjonens medlemmer, herunder kadettene, kan på denne måten bli mer robust når det gjelder å gjenkjenne og rapportere mulige hendelser og til og med angrep (Lockheed Martin, 2015). Kadettene bør derfor så tidlig som mulig få en forståelse for hvor lite som skal til for å trå feil i omgang med graderte systemer. På den andre siden kan det likevel bli et system uten hensikt. De fleste systemer ved skolen er ugraderte som også gjelder for Navkomps fasiliteter. Hvorfor da bruke tid og ressurser på prosedyrer og unødvendige rutiner rundt ugraderte systemer? Utdanning av operative kadetter er uansett en viktig modningsprosess som går gjennom flere år og det kan derfor argumenteres for at uavhengig av graderte systemer så må en slik tankegang læres i praksis. Det er derfor gode grunner til å benytte Sjøkrigsskolen som en arena for å utvikle denne tankegangen

[2] Kryptograd nivå 1 kan argumenteres for at tar for seg noe om datasikkerhet, men dette gis kun til enkelte linjer

før tjenesten starter, noe som kan tenkes å redusere tiden det tar før kadetten er operativ i stilling ute i marinen.

En faktor som trolig vil endre seg fra det inneværende kullet som ble undersøkt til neste kull, er kadettsammensetningen. Med dette mener vi sammensetningen av erfarne og uerfarne kadetter. Den nye skolemodellen satser tyngre på å ta opp yngre kadetter, helst personell uten forsvarserfaring rett fra videregående skole. En konsekvens av dette vil være at gjennomsnittserfaringen fra operativ tjeneste går ned. Denne nedgangen i erfaring vil trolig føre til at tverrsnittet av kadettene har mindre erfaring med omgang av kritiske og/eller graderte datasystemer før de begynner på Sjøkrigsskolen. De har altså ikke med seg en datasikkerhetskultur fra Forsvaret inn i skolegangen i like stor grad. På en annen side kan det argumenteres for at kadettene med sin unge alder har hatt mer med teknologi og de problemstillingene dette medfører å gjøre gjennom oppveksten, enn de eldre kadettene med lang fartstid i vår ordning i dag. Dette kan tenkes at gir dem en inngangsverdi til å ta datasikkerhetsmessige vurderinger uten å ha spesifikk militær utdanning på området. Det kan derimot også bety at deres jevnlige omgang med datasystemer på daglig basis har gitt dem et så dagligdags forhold til denne problemstillingen at det ikke tas på alvor.
Problemet vil med andre ord ganske enkelt bli å sørge for at alle følger samme operasjonsmønster og har like inngangsverdier for å sikre datasikkerheten på en forutsigbar måte.

### 5.4.3 Fravær av utdanning og opplæring

I delkapittel 5.4.2 nevner vi at det per dags dato ikke eksisterer et konkret utdanningsopplegg på temaet datasikkerhet. Dette kan medføre en usikkerhet rundt hva som er ønsket måte å opptre på, samt en uforutsigbarhet for ledelsen og de tekniske. Grunnen til dette er at brukeren av systemene i større eller mindre grad vil gjennomføre de tiltak en selv anser for å være tilstrekkelig for å ivareta god datasikkerhet. Det argumenteres for at et utdanningsopplegg vil kunne bedre datasikkerheten (Wråli, 2017).

Som vist i tabell 4 (O1-funnene) er dagens situasjon at det periodevis er stor aktivitet med disker på datamaskinene ved Navkomp og stor flyt av disker mellom de forskjellige stasjonene. Noen av disse maskinene er bak låste dører, mens andre er

tilgjengelige for alle som har tilgang til leiren og skolebygget. Ingen av maskinene, med unntak av AV-maskinen, er tilkoblet internett. Funnene rundt flyten av disker viser at de samme diskene tilkobles hyppig både på de åpent tilgjengelige og de innelåste maskinene. Dette er en fin måte å illustrere hvordan en ekstern trussel vil kunne nå maskinvare bak låste dører som ikke er koblet til internett. Ved å infisere de maskinene som er åpent tilgjengelig for å så la brukeren bære skadevaren med seg inn bak låste dører og infisere de låste maskinene uten viten og vilje kan en fiendtlig aktør utmanøvrere tekniske og fysiske hindringer. Om man skal knytte dette opp mot teorien om APT-er vil det da være mulig for slike aktører å identifisere brukere av systemet som for eksempel kadetter. Vi vet at det er mulig å oppdrive store mengder informasjon om enkeltpersoners kretser og liv gjennom åpne kilder (Fitton, Prince, Lacy, & Germond, 2015). Det kan da tenkes at denne informasjonen kan brukes til å finne mål, kartlegge for eksempel klasser og kull ved skolen og angripe gjennom private datamaskiner eller andre medium. Brukerens kompromitterte disk blir en inngangsvei for skadevare hvis denne kobles til maskiner på for eksempel Navlab, Teksim, Navsim eller skolefartøyene. Til tross for at det er en reell sjanse for slike angrepsveier er det likevel ikke sikkert det utgjør en trussel. Slike angrep vil muligens kreve mer ressurser enn det som vinnes og at kost-nytte-effekten er lav. Dette kan forøvrig være en årsak til en mangelfull datasikkerhetskultur fordi mange velger lettvinte og bekvemmelige løsninger ved bruken av disker og datasystemer. Det er likevel viktig for det forebyggende arbeidet å være klar over hvilke svakheter systemene innehar, inkludert menneskene som benytter systemet. Ut ifra funnene gjennom eksperimentet og den relevante teorien er det altså stor mulighet for at tendensen til bruk av disker hyppig og uten sikkerhetsrutiner kan utgjøre et sikkerhetshull. Dette kan i tillegg bidra til at god sikkerhetskultur forsømmes og mangelfull opplæring forekommer.

En kompromittering av planleggings- eller kartmaskinene på Navkomp og Navsim kan i verste fall føre til at besøkende personell fra operative avdelinger i Marinen vil kunne bli utsatt for eventuell skadevare og dermed kompromittering. Skadevare kan på denne måten havne på datamaskiner i operativ tjeneste. Muligheten er altså til stede for skolen fungerer som bakvei inn i andre avdelingers systemer.

Konsekvensen av slike kompromitteringer er potensielt mange og skadelige. En av de formene kan være informasjonsinnhenting. Ved å plante skadevare på en disk som er

innom mange forskjellige systemer vil denne skadevaren kunne innhente spesifikk data og sende denne tilbake til kilden hver gang den er koblet til en maskin med internettilgang. Dette er illustrert som en mild variant av ledd 7 i «Cyber Kill Chain»-modellen (figur 1). Dette kan brukes til å samle inn store mengder informasjon som aktøren kan bruke til å kartlegge handlemønster, relasjoner, operasjonskultur, hvor det er vanligst for marinefartøy å navigere, o.l. Desto større slike datamengder en aktør kan få tilgang til, desto mer gradert vil den totale datamengden kunne bli.
En mer aggressiv variant, men med potensielt større skadeomfang er planting av skadevare med sabotasje som mål. Dette er omtalt av Kristian Wråli og viser til at konsekvensen av rettede cyberangrep med sikte på å skade materiell og personell er svært høy og i verste tilfelle kan føre til tap av menneskeliv (Wråli, 2017).

### 5.4.4 Oppsummering

Gjennom funnene etter eksperimentet er det tydelig at vi kan si noe om maritim cybersikkerhet ved Sjøkrigsskolen og peke på mulige problemstillinger. Utfordringene ligger i at det ikke foreligger verken intensjoner eller rutiner omkring datasikkerhet og dette gjenspeiles i kadettenes handlemåte gjennom eksperimentet. Vi ser på det som en utfordring at det i liten grad er kommunikasjon mellom skoleledelsen og kadettene om hva som forventes av datasikkerhetskultur.
Gjennom teori og drøfting er det pekt på mer spesifikk utdanning, oppfølging og fokus på temaet som mulige tiltak for å endre kulturen. Her foreligger problemstillinger rundt hvordan eventuell utdanning kan gjennomføres med tanke på en felles undervisning eller ikke. Det vil også foreligge en underliggende problemstilling rundt kost-nytte-effekten av en slik undervisning.
Per i dag er det påvist gjennom forsøk at det er stor aktivitet med ugraderte lagringsenheter mellom skolens datamaskiner. Den store flyten kan utgjøre en potensiell trussel hvis sikkerhetshullene utnyttes av aktører som for eksempel APT-er. Konsekvensene av dette er også påvist å være svært alvorlige og i ytterste konsekvens føre til store materielle skader og tap av menneskeliv.

# 6 Konklusjon med anbefaling

Gjennom problemstillingen ønsket vi spesifikt å se på hvordan en enkel operasjonsprosedyre ville påvirke et utvalg kadetter ved Sjøkrigsskolen. Denne effekten ønsket vi å studere gjennom å utføre et kvasi-eksperiment.

Eksperimentets O1 viste at utvalgets bruk av AV-scanning i utgangspunktet var minimal og det er konkludert gjennom analyse og drøfting at dette resultatet i noen grad kan generaliseres til hele Sjøkrigsskolen.
Eksperimentets observasjon 2 baseres på innføringen av en operasjonsprosedyre med påfølgende planleggingsfase før en større navigasjonsøvelse. Prosedyren ble gitt muntlig og skriftlig til halve utvalget, eksperimentgruppen. Totalt sett endret 4 av 19 gyldige kandidater atferd, hvorav tre tilhører eksperimentgruppen og én tilhører kontrollgruppen. To kandidater har gjennomført prosedyren på en korrekt måte. Vi har identifisert at det kan være et stort antall ukjente tredjepartsfaktorer med i bildet som gjør det vanskelig å peke på en soleklar grunn til endring i atferd hos kandidatene. Effekten av vår prosedyre kan avhenge av flere faktorer. Vi antar at faktorer som vår autoritet som utgiver, ansvarliggjøring av kadettene, oppfølging, kompetanse på feltet samt forståelse for viktigheten av datasikkerhet er mekanismer som kan ha påvirket effekten. Vi tror derfor at den måten vi implementerte prosedyren på manglet vesentlige elementer av faktorene nevnt over, som kan ha ført til at effekten ble dårligere enn ønsket.

Gjennom drøftingen mener vi at den dårlige effekten av en ny prosedyre eller sikkerhetsrutine kan skyldes manglende fokus på datasikkerhetskultur. Siden funnene er såpass entydige fremstår det som svært sannsynlig at Sjøkrigsskolen som utdannende institusjon innehar mange av de samme trekkene som kadettene viser gjennom eksperimentet. Med andre ord kan atferden trolig generaliseres til hele institusjonen. Om dette stemmer kan det potensielt kreve mye tid og ressurser for å endre samt etablere et varig miljø og en kultur som fremmer god datasikkerhet.

Vi anbefaler at skolens ledelse fokuserer på ytterligere undersøkelser, forskning og utredning på hvorvidt et fokus på maritim cybersikkerhet bør prioriteres ved Sjøkrigsskolen som utdanningsinstitusjon. Fagpersonell bør konsulteres om nye rutiner skal etableres og det må fokuseres på å fremme en bedre datasikkerhetskultur i hele

avdelingen. I lys av funnene og drøftingene som er gjort mener vi at det er viktig å inkludere kadettene i denne utviklingen i den hensikt å skape en ansvarliggjørelse og et eierskap hos kadettmassen. Målet med dette er å oppnå at hver enkelt person på Sjøkrigsskolen som avdeling, bidrar, vurderer og tar ansvar for datasikkerheten. Evalueringer av dette bør derfor omfatte skolen som en helhet der kadetter og stabsansatte er likestilte operatører av systemene. På denne måten vil alle ved avdelingen være likestilte aktører på cyberdomenet og dette kan fremme hver enkelt persons ansvar og eierskap til datasikkerheten ved Sjøkrigsskolen.

# Bibliografi

Cook, T. D., & Campbell, D. T. (1979). *Quasi-Experimentation - Design & Analysis Issues for Field Settings.* Boston: Houghton Mifflin Company.

Dahl, Ø., & Befring, E. (2010, Okt 12). Hentet fra Digitale læremidler for videregående opplæring: https://ndla.no/nb/node/21800?fag=6118

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet.* Fornyings-, administrasjons, og kirkedepartementet . Hentet fra www.regjeringen.no: https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

Fitton, O., Prince, D., Lacy, M., & Germond, B. (2015). *The Future of Maritime Cyber Security.* Lancaster University.

Goward, D. (2017, Nov 7). *The Maritime Executive*. Hentet fra https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.d5uUHJw

Hareide, O. S., Jøsok, Ø., Ostnes, R., Helkala, K., & Lund, M. S. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*(Accepted, in publication).

Jacobsen, D. I. (2010). *Hvordan gjennomføre undersøkelser - Innføring i sammfunnsvitenskapelig metode.* 4630 Kristiansand: Høyskoleforlaget.

Lockheed Martin. (2015). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Hentet April 2018 fra Lockheedmartin.com: https://lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Marquet, L. D. (2012). *Turn the Ship Around.* New York 10014, New York: Penguin Group.

Røislien, H. E. (2018, April 13). Når tid og sted ikke betyr noe lenger: Hva cybersikkerhet og cyberforsvar egentlig er. *Foredrag under Den Norske Atlanterhavskomités kurs i internasjonal politikk*. Laksevåg.

*Scalelive.com*. (2016). Hentet fra https://www.scalelive.com/nonequivalent-control-group-design.html

Wråli, K. (2017). *Maritim Cybersikkerhet - Operasjonelle konsekvenser ved maritime cyberangrep.* Forsvarets Ingeniørhøgskole. Jørstadmoen: Forsvaret.