FORSVARET
Forsvarets høgskole

# Kartlegging av maritime hybride trusler

*Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet?*

**Stian Schnelle**

Masteroppgave

Forsvarets høgskole

Høst 2018

# Forord

Denne masteroppgaven er blitt til som en del av stabs- og masterstudiet ved Forsvarets Høgskole 2017/2018. Arbeidet med oppgaven har vært utrolig givende, og har gitt muligheter for fordypning i et komplekst tema som har gitt ny kunnskap og innsikt, både faglig og personlig. Det er en lang, og til tider krevende reise, som nå går mot slutten.

Studien hadde ikke vært mulig å gjennomføre uten svært verdifulle bidrag underveis. For at oppgaven fremstår som den gjør rettes en spesiell takk til min biveileder, sjefsforsker ved FFI, Frank Bruntland Steder. Uten dine gode råd og uvurderlige bidrag gjennom hele prosessen ville ikke denne oppgaven vært mulig å gjennomføre. Jeg vil også rette en stor takk til hovedveileder Palle Ydstebø som også har gitt svært verdifulle bidrag underveis, og sørget for at prosjektet har holdt stødig kurs hele veien.

Oppgavens analysedel er unik i norsk kontekst. Samarbeidet med Naval Postgraduate School (NPS) i Monterey var essensielt for å høste erfaringer og innsikt i forskningsmetoder som kun er benyttet et fåtall ganger tidligere. En spesiell takk går til Dr. Wayne Porter, Rob Schroeder og Christopher Callaghan ved Littoral Operations Center og CORE Lab for særdeles viktig støtte og bidrag i forbindelse med prosjektet. En stor takk til Dagfinn Vatne, FFI sin liaison til NPS. Mange takk for dine særdeles gode innspill og bidrag underveis i prosessen. Jeg vil også uttrykke min takknemlighet overfor tidligere forsvarssjef Sverre Diesen som stilte opp til intervju, og delte av sin kunnskap og innsikt om hybrid krigføring. Videre går en takk til Admiral James Stavridis, som tok seg tid til å bidra med sitt syn på oppgavens vinkling.

Tusen takk rettes også til dere som har lest oppgaven og gitt verdifulle tilbakemeldinger. En spesiell takk Marius Thormodsen som åpnet viktige dører for meg i prosessen med valg av tema for oppgaven, og din rolle som verdifull sparringspartner underveis i prosjektet.

Sist, men ikke minst vil jeg rette en takk til min samboer Lene og våre to barn Herman og Lukas for tålmodigheten deres. Takk for at dette var mulig!

# Sammendrag

Denne oppgaven handler om hvordan stordata og sosial nettverksanalyse (SNA) for kartlegging av maritime hybride trusler kan øke situasjonsbevisstheten i det maritime domenet. Hybrid krigføring kjennetegnes ved en koordinert bruk av statens maktinstrumenter (militære, politiske, økonomiske, sivile og informasjonsmessige)[1] der irregulære virkemidler i stor grad har tatt over rollen til regulære militære maktmidler. Denne helhetlige tilnærmingen til konflikt har blitt aktualisert med bakgrunn i Russlands handlinger på Krim. Hensikten til en hybrid aktør er å skape en situasjon preget av tvetydighet og tvil, slik at det oppstår en uklar gråsone mellom krig og fred.

I Sør-Kina-havet har spenningen økt mellom Kina og USA. Kinas oppbygging av kunstige øyer, og etableringen av en maritim «milits» bestående av sivile fartøyer anses å være svært utfordrende. Russisk maritim doktrine anerkjenner også sivile fartøyer som viktige bidragsytere til russisk projeksjon av sjømakt. Ser vi dette i en sammenheng, fremmer dette et behov for større fokus på kartlegging av aktører og mulige nettverk i det maritime domenet. Maritim situasjonsbevissthet i dag fokuserer på bruk av tradisjonelle disipliner som etterretning, overvåkning og rekognosering. Det lite tilgjengelig forskning på maritime nettverksstrukturer. Denne oppgaven besvares med kombinert metode der en omfattende kvalitativ litteraturstudie legges til grunn for og kombineres med en kvantitativ stordata- og nettverksanalyse av historiske Automatic Identification System data (AIS).

SNA kartlegger mønster og relasjoner mellom sosiale aktører og koblingen mellom aktørene danner et nettverk som videre analyseres. Hensikten med studiens analysedel er å gi et «proof of concept» for at bruk av AIS-stordata og SNA til kartlegging av maritime hybride trusler kan bidra til økt situasjonsbevissthet. Fokuset for oppgaven er kommersielle russiske fartøyer i norske interesseområder. Gjennom bruk av stordata og SNA har algoritmisk filtrering av store mengder data kombinert med bruk av åpne kilder og databaser bygget maritime nettverksstrukturer. Studiens hovedkonklusjon er at stordata og sosial nettverksanalyse vil kunne bidra til økt maritim situasjonsbevissthet, inkludert kartlegging av maritime hybride trusler, forutsatt at det benyttes som et supplement til eksisterende prosesser og systemer.

[1] Instruments of power. Oversatt fra MPECI – military, political, economic, civil, information

# Summary

This thesis analyzes use of big data and social network analysis as a contribution to increase Maritime Domain Awareness (MDA) by mapping maritime hybrid threats. Hybrid Warfare takes a coordinated, systematic and comprehensive approach using military, political, economic, civil and informational instruments of power (MPECI) to achieve the state`s ends. Hybrid threats are designed to deliberately blur and blend to create a high degree of uncertainty and unpredictability, caused by increased importance of the non-military measures and irregular tactics which in many ways has surpassed the importance of conventional military measures. Having attracted new attention in the aftermath of the Ukraine crisis, such grey-zone activities between war and peace can prove challenging to detect.

The situation in the South-China Sea, where China is conducting terra-forming operations to build artificial islands combined with the establishment of a maritime militia of civilian merchant vessels and fishing vessels, is challenging the USA. This, in conjunction with the Russian Maritime Doctrine which regognizes civilian vessels as contributors to russian projection of sea power, it highlights a need to focus on identification and mapping of actors and networks in the maritime domain. Very little available social network research has been conducted on mapping of possible maritme hybrid threats in the maritime domain. This thesis uses a mixed methods approach where the first part creates a qualitative foundation for the combination of the quantitative analysis in the second part. The thesis considers how to infer a social network based on location information captured from historical Automatic Identification System (AIS) data.

SNA provides the capability to detect and analyze patterns of social ties between actors, and how these create structures and networks which again can be investigated. The analysis in this thesis will be conducted as a «proof of concept», combining big data and SNA for the mapping of hybrid threats to increase MDA. The main scope for the thesis has been mapping of commercial russian networks. By creating customized data structures, and by implementing algorithms filtrering and data combined with open source and database investigation the social networks were designed. The thesis has identified behavioural patterns and maritime networks by identifying ships, their owners, and geo-locations. The main finding of the thesis is that a combination of big data and social network analysis can provide added value to the MDA process, including identification of possible hybrid threats.

# Innholdsfortegnelse

## Forkortelser

| | |
|---|---|
| **AIS** | Automatic Identification System |
| **COG** | Course over Ground |
| **DTG** | Dato-tidsgruppe |
| **GPS** | Global Positioning System |
| **FFI** | Forsvarets Forskningsinstitutt |
| **IMO** | International Maritime Organization |
| **MDA** | Maritime Domain Awareness |
| **MID** | Maritime Identification Digit |
| **MMSI** | Maritime Mobile Service Identity |
| **MPECI** | Military, Political, Economic, Civilian, Informational |
| **MSA** | Maritime Situational Awareness |
| **NPS** | Naval Postgraduate School |
| **PMESII** | Political, Military, Economic, Social, Information, Infrastructure |
| **POI** | Point of Interest |
| **SNA** | Social Network Analysis |
| **SOLAS** | Safety Of Lives At Sea |
| **SOG** | Speed over Ground |
| **UTC** | Universal Time Coordinated |

# 1 Innledning

*«Norge er en maritim og arktisk nasjon med globale maritime interesser. Vårt velferdsgrunnlag og nasjonaløkonomi er i stor grad knyttet til de maritime næringer» (Forsvaret, 2015a, s. 3)*

Det eksisterer i dag statlige og ikke-statlige aktører som gjennom en rekke åpne og skjulte aktiviteter utfordrer både nasjoners og institusjoners sårbarheter. Den russiske annekteringen av Krim i 2014 og den stadig pågående destabiliseringen av det østlige Ukraina viser endring i russisk politikk og deres tilnærming til konflikt. Tilnærmingen kjennetegnes av at andre virkemidler enn konvensjonell militærmakt dominerer krigføringen (Diesen, 2018, s. 8). Dette utfordrer NATO og den tradisjonelle tankegangen rundt kollektivt forsvar, og forpliktelsene alliansen har i forbindelse med NATOs artikkel 5. De mest åpenbare handlingene, bruk av grupper av «små grønne menn», var bare en del av et sammensatt og vidt spekter av virkemidler som alle søkte å tjene russiske strategiske interesser. Hva var det vi egentlig vi var vitne til? I vesten har begrepet «hybrid krigføring» eller «*New Generation Warfare*» blitt brukt i om denne «nye» tilnærmingen til konflikt. Begrepet søker å forklare dette komplekse fenomenet som har gitt en rekke nye, tidligere uforutsette, sikkerhetsutfordringer. Paralleller kan trekkes til Sør-Kina-havet, der Kina bruker kystvaktfartøyer sammen med sivile fartøyer som et ledd i pågående operasjoner der hensikten er å utvide sitt territorium og territorialfarvann ved å bygge kunstige øyer (Johnson, 2018, s. 142). Kinas handlinger understreker også viktigheten av å fokusere på trusselen i det maritime domenet.

Etter NATO Wales Summit i 2014 ble hybrid krigføring beskrevet som «a wide range of overt and covert military, paramilitary, and civilian measures...employed in a highly integrated design.» (NATO, 2014b). Det har gradvis blitt erkjent at russisk tilnærming til konflikt verken er ny eller unik, men en utvikling av eksisterende tankegang, nå styrket av den teknologiske utviklingen. Russland innehar i dag en rekke kapasiteter som kan utfordre både NATO og dets regionale partnere, også i det maritime domenet. For å kunne håndtere det nye trusselbildet kreves det at vi overvåker og forstår russisk aktivitet.

Norge ligger sentralt til for det russiske *bastionsforsvaret*, som i tillegg til russiske ubåters patruljeområder i Barentshavet (bastionen) i bredeste forstand også inkluderer Norskehavet og Atlanterhavet. Videre har Norge vesentlige interesser i disse områdene hva angår olje-, gass- og fiskerinæring. I en konflikt vil det være en prioritert oppgave for Russland å beskytte disse områdene (Forsvarsdepartementet, 2015, s. 20). Dette gjør oss sårbare. Håndtering

av hybride trusler skal ikke nødvendigvis løses av Forsvaret alene, men krever en helhetlig respons som innebærer at samfunnets ressurser må bidra til samlet innsats av nasjonale kapasiteter (FD/JD, 2015, s. 19).

Russlands handlinger i Ukraina demonstrerer et behov for økt forståelse av hvilke virkemidler som potensielt kan benyttes mot oss i våre interesseområder. Mye av fokuset i litteraturen rundt hybride trusler har i stor grad dreid seg om bruk av landstyrker kombinert med andre virkemidler for påvirkning. Den potensielle trusselen medfører også et økt behov for å forstå hva som skjer, eller kan skje i det maritime domenet. Forsvarets doktrine for maritime operasjoner erkjenner at også Norge kan bli utsatt for hybride trusler, i en fase hvor hensikten er å tilsløre faktiske forhold for å for eksempel unngå at NATOs artikkel 5 blir utløst (Forsvaret, 2015a, s. 29). Norges havområder er syv ganger så stort som landområdene. Deler av Norges sjøområder er også tett traffikert av sivil skipsfart, og således velegnet til bruk og iverksetting av skjulte irregulære virkemidler. Russisk maritim doktrine anerkjenner både russiske militære og sivile fartøyer som en viktig bidragsyter til russiske myndigheters projeksjon av sjømakt. Bruk av sivile fartøy, og spesialstyrker med amfibiekapasitet er identifisert som mulige trusler, og er overførbare til våre nærområder (Hicks, 2018, s. IV).

Utviklingen av den helhetlige tilnærmingen til konflikt vi observerer fra russisk side påvirker hvordan vi analyserer og vurderer trusselbildet. Basert på hvordan den sikkerhetspolitiske situasjonen har utviklet seg, er det viktig å vurdere nye former for analyse og kartlegging av de hybride truslene i det maritime domenet. God situasjonsbevissthet i våre nærområder danner grunnlaget for at politisk og militær ledelse kan fatte gode beslutninger og optimal anvendelse av Forsvaret. Effektiv overvåking gjennom innhenting, sammenfatting, analysering og videreformidling av informasjon vil kunne bidra til god situasjonsforståelse både nasjonalt, og i NATO (Forsvarsdepartementet, 2016, s. 24). Hensikten med denne studien er derfor å belyse utfordringer knyttet til hybride trusler i det maritime domenet, og hvordan vi kan møte disse utfordringene.

Fokuset på hybrid krigføring og konflikter i gråsonen (uklar tilstand mellom krig og fred) fremhever et behov for å fokusere mer på identifikasjon og lokalisasjon av nøkkelaktører i «*mørke sosiale nettverk*» (nettverk som ikke opererer med transparens) i det maritime domenet. Sosial nettverksanalyse (SNA) har tradisjonelt sett blitt benyttet i landdomenet blant annet for å kartlegge terroristnettverk, cybernettverk og narkotikanettverk. Det er kun nylig forskning på hvordan metoden kan anvendes mot *mørke nettverk* eller *grå nettverk* (nettverk som opererer delvis åpent) i det maritime domenet (Porter, Warren & Schroeder, 2018, s. 1). Denne oppgaven vil undersøke hvordan vi ved bruk av *stordata* og metoder fra *sosial nettverksanalyse* kan oppnå

en *bedret maritim situasjonsbevissthet* i norske interesseområder og hvordan vi i et strategisk perspektiv kan hindre disse nettverkene i å utnytte sine kapasiteter i gråsonekonflikter. Ulikt tradisjonelle virkemidler, er SNA en metode som brukes for å analysere strukturen i relasjonen mellom aktører enten det dreier seg om individer, fartøyer eller organisasjoner (Everton, 2012, s. 5). Analysen av sosiale koblinger og interaksjon mellom ulike aktører kan hjelpe oss til å forstå hvem som er viktige i et nettverk, hvilken rolle de ulike aktørene har, og hvilke eventuelle undergrupper og noder som er tett sammenknyttet (Golbeck, 2013, s. 1). Disse nettverkene kan i lys av russisk maritim doktrine utnyttes i et hybrid scenario. Tilknyttet det russiske statsapparatet kan maritime nettverk brukes til å påvirke det maritime domenet i våre interesseområder i favør av russiske strategiske interesser.

# 1.1 Problemstilling og avgrensning

«*Åpne og tillitsbaserte vestlige samfunn er sårbare og dårlig forberedt i møte med de hybride virkemidlene» (Forsvarsdepartementet, 2015, s. 33).*

Oppgavens målsetting er å bidra til økt kunnskap om hvordan bruk av stordata og SNA kan danne et analytisk rammeverk for å få en dypere og mer presis situasjonsbevissthet i det maritime domenet.

Problemstillingen for oppgaven er:

***«Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet?»***

Problemstillingen vil bli analysert ved å belyse følgende forskningsspørsmål:

*Forskningsspørsmål 1: Utgjør mørke eller grå maritime nettverk som en del av «russisk helhetlig tilnærming til konflikt» en reell utfordring i norske interesseområder?*
*Forskningsspørsmål 2: Hvordan kan maritime hybride trusler utfordre vår maritime situasjonsbevisshet?*
*Forskningsspørsmål 3: Hvordan kan sosial nettverksanalyse (SNA) som metode benyttes for å kartlegge maritime hybride trusler?*

Denne oppgaven tar for seg hvordan bruk av stordata, analysert med metoder brukt i sosial nettverksanalyse, kan benyttes i det maritime domenet for å oppdage aktører som opererer i helt eller delvis skjulte maritime nettverk. Slike nettverk kan ha ulike former og tjene ulike hensikter over et vidt spekter som for eksempel narkotikatrafikk og våpensmugling. Studien vil primært

fokusere på russiske maritime nettverk som potensielle hybride trusler i lys av maritim hybrid krigføring og russisk maritim doktrine. Oppgavens analysedel vil bli presentert som et «proof of concept» for hvordan metoder fra SNA kan bidra til å avdekke maritime nettverksstrukturer og slik bidra til økt situasjonsbevissthet i det maritime domenet. Analysen omfatter historiske data fra 2014 og 2017. Dette valget er gjort av to årsaker. Den første er grunnet begrensninger i oppgavens omfang. Den andre er for å undersøke om man kan identifisere utviklingstrekk over tid mellom det samme året Russland annekterte Krim, og frem til i dag. Til tross for oppgavens fokus på maritime nettverk, er det viktig å presisere at disse må sees i sammenheng med hele spekteret av konvensjonelle og ikke-konvensjonelle virkemidler i den helhetlige tilnærmingen som Russland har vist at de har hatt i sin verktøykasse.

Denne oppgaven har som ambisjon å undersøke om bruk av stordata og SNA kan benyttes til kartlegging og mulig identifikasjon av maritime hybride trusler i en norsk maritim kontekst for å skape økt maritim situasjonsbevissthet. Oppgaven har imidlertid ikke som ambisjon å gjennomføre en fullstendig analyse av samtlige potensielt skjulte nettverk i norske interesseområder. Det er også relevant å understreke at oppgaven omhandler SNA som et mulig bidrag til eksisterende metoder og kapasiteter for overvåkning av norske interesseområder, og at metodikken alene ikke er tilstrekkelig for kartlegging av trusler, eller for å skape en god situasjonsbevisshet.

## 1.2 Hypotese

Bruken av irregulære virkemidler til fordel for konvensjonelle maktmidler har fått økt betydning i moderne konflikter. Både Diesens «Lavintensivt hybridangrep på Norge i en fremtidig konflikt» (Diesen, 2018) og den såkalte «Gerasimov doktrinen» (Bartles, 2016), anerkjenner dette. Dette får konsekvenser også i det maritime domenet, hvor etterretning og overvåkning – førstelinjeforsvaret – er kritiske for forsvarsevnen (FD/JD, 2015, s. 72).

Min hypotese er at norsk evne til å skape tilstrekkelig maritim situasjonsbevissthet, i lys av russisk helhetlig tilnærming til konflikt, ikke er innrettet for å møte hybride trusler i det maritime domenet. Vi trenger å tenke nytt rundt disse utfordringene.

## 1.3 Bakgrunn og sentrale begreper

For å skape et felles utgangspunkt og forståelse av begrepsapparatet som er benyttet i oppgaven, er det innledningsvis hensiktsmessig å gi en kort beskrivelse av disse:

### Stordata

AIS (Automatic Indentification System) er i Viventos rapport til kommunal og moderniseringsdepartementet «Kartlegging og vurdering av stordata i offentlig sektor» nevnt

som en viktig stordatakilde med et stort potensiale (Vivento, 2015, s. 33). Datasettene som er benyttet i oppgaven er hentet inn fra Kystverkets AIS database og inneholder eksempelvis 5 terrabyte med data bare for 2017. Dette utgjør rundt 20 millioner rader med data hver dag. Slike mengder informasjon krever andre statistiske analysemodeller enn tradisjonelle analyser (Lanestedt, 2016, s. 52). Som konsept omfatter stordata hele «verdikjeden» for data; produksjon, lagring, prosessering, analyse og visualisering av resultater. I denne oppgaven legges følgende definisjon hentet fra Viventos rapport til grunn for begrepet stordata:

> *«Stordata er analyse av massive samlinger av data («volume»), med stor variasjon i datakilder og formater («variety»), hvor datasettet oppdateres med høy frekvens («velocity») og hvor grunnlagsdataenes opprinnelse og kvalitet er avklart («veracity») og hvor analysen av datasamlingene gir økt verdi i forhold til hva datakildene enkeltvis ga («value»)»*. (Vivento, 2015, s. 15)

## Sosial Nettverksanalyse (SNA)

Sosial nettverksanalyse er en metode som har til hensikt å kartlegge mønster mellom sosiale aktører ved å studere relasjonene mellom aktører eller sosiale enheter heller enn egenskapene ved disse (Everton, 2012, s. 5). Ved å konsentrere oppmerksomheten til båndene mellom sosiale enheter fremfor kvalitetene disse måtte inneha, er det mulig å tenke nytt rundt hvilke muligheter og begrensninger som skapes av måten sosiale relasjoner er organisert på (Raab & Milward, 2003, s. 417). I denne studien fokuseres det på identifikasjon av fartøyer, eierstrukturer og interesseområder (geolokasjoner) ved bruk av åpne kilder og databaser, og operasjonalisering av disse som noder i fremstillingen av det sosiale nettverket. Begrepet nettverk brukes i denne sammenhengen om et system av aktører, hvor systemet har helt spesifikke kjennetegn eller trekk. SNA springer ut fra teorier og metoder som antar at aktørers adferd (individer, grupper eller organisasjoner) er påvirket av hvilke bånd de deler med andre aktører og de nettverkene de er en del av (Everton, 2012, s. 5). Et eksempel fra forskningen er for eksempel kartleggingen av nettverket som stod bak terrorangrepet i New York 11. september 2001 (Krebs, 2002).

## «Mørke og grå maritime nettverk»

Begrepet «dark networks» (oversatt til mørke nettverk) er nettverk som per definisjon forsøker å holde seg skjult eller fordekt (Everton, 2012, s. 399). Raab og Milward definerer *mørke nettverk* som «illegale og skjulte» (Raab & Milward, 2003, s. 419). Oppgaven forholder seg til m*ørke maritime nettverk* (nettverk som ikke opererer med transparens) og *grå nettverk* (nettverk som opererer delvis åpent) i det maritime domenet i tråd med Porters bruk av begrepet (Porter et al., 2018, s. 1). Begrepet er tidligere brukt om terrornettverk, gjenger, smuglere og andre kriminelle

organisasjoner (Cunningham, Everton & Murphy, 2016, s. xvii). I denne studien defineres «mørke maritime nettverk» som *maritime nettverk, som med bruk av formelle eller uformelle bånd, opererer fordekt eller delvis fordekt i norske interesseområder og som potensielt kan benyttes som irregulære virkemiddel for å oppnå sine målsettinger*.

## Maritim situasjonsbevissthet

Kompleksiteten i norske interesseområder er stor og karakteriseres blant annet av geografiske forhold som både utstrekning og nærhet til Russland, stor andel sivil kommersiell trafikk, og tilstedeværelse av russiske militære styrker. Forsvaret er avhengig av god situasjonsbevissthet i disse områdene for å kunne fatte gode beslutninger og for å kunne anvende Forsvarets ressurser best mulig. I proposisjonen til gjeldende langtidsplan for forsvarssektoren, Stortingsproposisjon 151S, er Norges evne til å etablere og vedlikeholde situasjonsforståelse i norske nærområder regnet som en forutsetning for å kunne møte kriser på en effektiv måte (Forsvarsdepartementet, 2016).

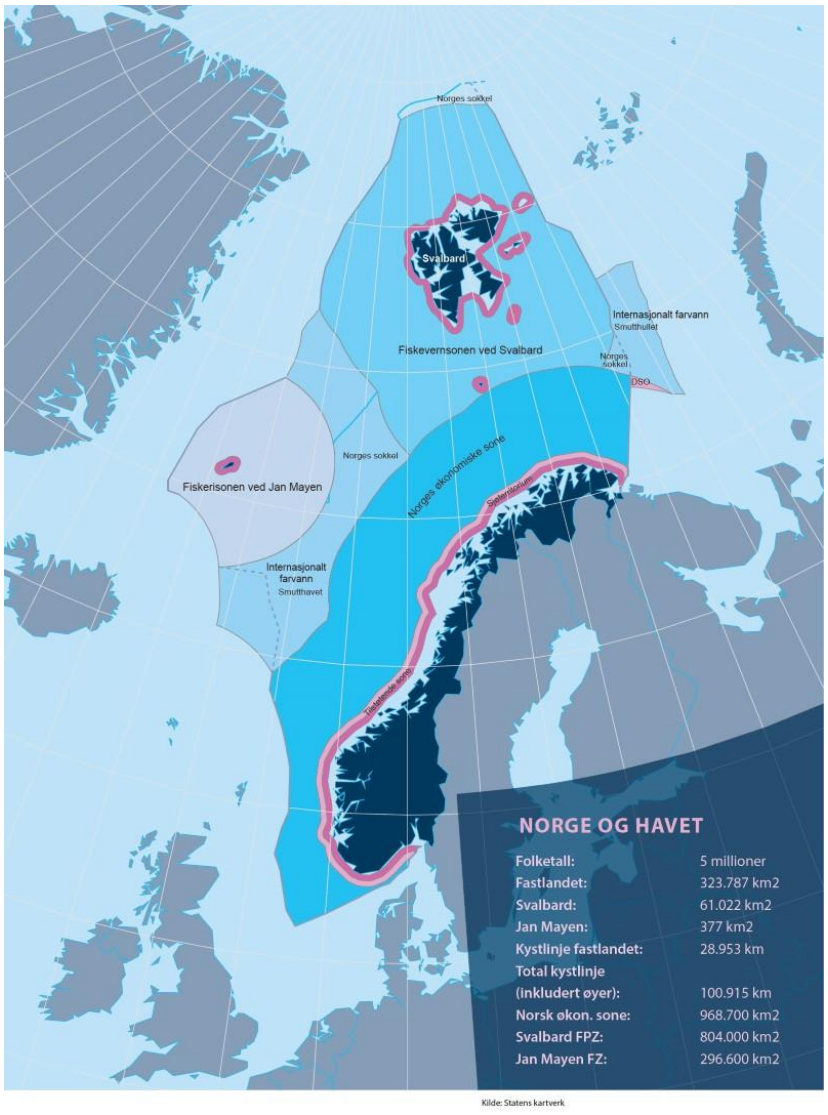
Forsvarets Fellesoperative Doktrine (FFOD) definerer *situasjonsbevissthet* som forståelsen av alle forhold i og omkring operasjonsområdet som er nødvendig for å fatte informerte beslutninger (Forsvarsstaben, 2014, s. 230). NATOs begrep, *Maritime Situational Awareness (MSA)* er en variant av *Maritime Domain Awareness* (*MDA*) som i amerikansk er doktrine definert som: *«The effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of a nation or region»* (Hicks, 2018, s. IV). Oversatt kan MDA - *Maritim Situasjonsbevissthet* deles inn i tre nivåer (Forsvaret, 2015a, s. 133):

1. Situasjonsoppfattelse av observerte data.
2. Situasjonsforståelse ved integrasjon av data og bevisstgjøring av betydningen for det som skjer.
3. Situasjonsprediksjon innebærer en evne til å forutse hendelser basert på gjenkjenning av tidligere mønster.

## Norske interesseområder

Norges viktigste strategiske interesseområde er nordområdene, som utgjør 80 prosent av Norges havområder. For å kunne sikre et nasjonalt beslutningsgrunnlag må vi ha evne til å etablere og vedlikeholde situasjonsbevissthet i disse områdene. Dette er knyttet opp mot Forsvarets oppgaver i den hensikt å skaffe rettidig beslutningsgrunnlag for både politisk ledelse og ledelsen i Forsvaret (Forsvarsdepartementet, 2016, s. 24). Norges 200 nautiske mil økonomiske soner rundt det norske fastland (NØS) ble opprettet med virkning fra 1. januar 1977. Fiskevernsonen

ved Svalbard ble opprettet 15. juni samme år. Den siste sonen, fiskerisonen ved Jan Mayen, ble opprettet med virkning fra 29. mai 1980. Alle tre soner er opprettet i medhold av lov av 17. desember 1976 om Norges økonomiske sone, også kalt soneloven (Regjeringen, 2014). Dette utgjør Forsvarets ansvarsområde. Norske interesseområder strekker seg ut over dette, og vil grunnet graderingsnivå ikke bli beskrevet nærmere i denne oppgaven.




Figur 1.1 (regjeringen.no)

## 1.4 Oppgavens struktur

Oppgaven er todelt. Første del består av kapittel to til seks og utgjør oppgavens teoretiske rammeverk. Andre del består av kapittel syv til åtte, og består av den konseptuelle tilnærmingen, analyse og drøfting av resultater.

***Kapittel to*** vil redegjøre for oppgavens valg av forskningsdesign, metodisk fremgangsmåte, og datainnsamling.

***Kapittel tre*** vil analysere sentrale utviklingstrekk rundt russisk helhetlig tilnærming, og russisk maritim doktrine. Dette er viktig for oppgaven fordi innsikt i utviklingstrekk i væpnede konflikter og hva som er den dimensjonerende trusselen for Norge, er en premissgiver for den sosiale nettverksanalysen (SNA) i oppgavens andre del.

***Kapittel fire*** redegjør for hvordan vi i dag bygger vår maritime situasjonsbevissthet, hvilke aktører som deltar, og hvordan prosessen foregår. Dette er relevant for vurderingen av hvordan situasjonsbevisstheten i det maritime domenet kan utfordres, og om SNA kan være en relevant metode for å øke denne.

***Kapittel fem*** beskriver grunnleggende aspekter ved konseptet og datagrunnlaget for studiens hovedkilde, Automatic Identification System (AIS). Denne delen viser også til mulige feilkilder, samt tidligere studier hvor AIS er benyttet som primær datakilde.

***Kapittel seks*** er en teoretisk gjennomgang av SNA og fokuserer på sentrale aspekter og konsepter ved nettverksteori og SNA. Dette er relevant for å forstå teorien bak den kvantitative analysen i kapittel åtte.

***Kapittel syv*** redegjør for dataseleksjon og strategien for oppgavens analyse, og hvordan modellering av nettverk og presentasjon av resultater vil bli gjennomført. Her beskrives også programmeringsspråket R, og de viktigste applikasjonene og algoritmene som er benyttet i analysen.

***Kapittel åtte*** utgjør oppgavens analysedel. Hensikten med kapittelet er å er å gi et «proof of concept» for at bruk av AIS-stordata og sosial nettverksanalyse til kartlegging av maritime hybride trusler kan gi økt situasjonsbevissthet. Historiske data fra 2014 og 2017 vil analyseres, presenteres, og til slutt sammenlignes.

# 2 Metode og kilder

Forenklet kan man hevde at skillet mellom *kvalitative* og *kvantitative* metoder ofte blir forklart med at der den ene metoden bruker ord, bruker den andre metoden tall (Creswell, 2014, s. 4). Oppgavens design er en *teoretisk fortolkende casestudie*. Denne formen for design tillater forskeren å utvikle en dybdeanalyse av caser, hendelser, aktiviteter, prosesser som er avgrenset i tid (Creswell, 2014, s. 14).

*Kvalitativ forskningsmetode* forenkler prosessen med å studere komplekse og uklare problemstillinger ved å gjøre det lettere å gå i dybden. I en kvalitativ tilnærming bruker man ulike metoder for å undersøke et problem sin kontekst for deretter å tolke dette for å oppnå en øket forståelse (Creswell, 2014, s. 4). Utfordringen er å overføre resultater fra slike design til andre situasjoner (Busch, 2013, s. 53). Fokuset er altså ikke på generaliserbarhet, men på gyldighet av analysene.

*Kvantitative studier* gjør det lettere å håndtere store datamengder, såfremt man har klart definerte og avgrensede teoretiske modeller (Busch, 2013, s. 53). Den kvantitative tilnærmingen tester objektive teorier ved å se på forholdet mellom variabler som er målbare, slik at data kan bli analysert ved bruk av statistiske metoder (Creswell, 2014, s. 4).

*Blandet metode.* Oppgaven vil bli gjennomført med bruk av *både kvalitativ* og *kvantitativ* metode, såkalt *blandet metodebruk*. Dette innebærer integrering av både kvalitative og kvantitative data for å oppnå en dypere forståelse av oppgavens problemstilling enn bruk av metodene hver for seg ville gjort (Creswell, 2014, s. 4). Oppgaven studerer først *kvalitative* data og beskriver således hvordan de kvalitative funnene er relevant for den *kvantitative* delen av studien. Det er en målsetting at kapitlene 2 til 5 skal bidra som et teoretisk og empirisk grunnlag for konstruksjonen av verktøyet for og gjennomføring av analysen i kapittel åtte. Creswell omtaler denne metoden som sekvensielt utforskende design (Creswell, 2014, s. 225). Hensikten er å først identifisere de bakenforliggende årsakene til hvorfor vi bør være årvåkne for den type maritime nettverk som studien omhandler (hva spørsmål). Videre er et av hovedpoengene med studien å analysere om bruk av stordata og SNA som metode kan øke vår evne til å kartlegge og forstå disse nettverkene (hvordan spørsmål).

Valget av metode ble gjort fordi metodene utfyller hverandre på en god måte. Oppgavens første del har en teoretisk fortolkende tilnærming til begrepet *hybrid krigføring* og *russisk maritim doktrine*. Hensikten med den kvalitative litteraturgjennomgangen er å analysere hvorvidt *russisk helhetlig tilnærming* og *russisk maritim doktrine* er en reell utfordring, og eventuelt hvordan dette kan komme til uttrykk i norske interesseområder. Studiens bruk av teori og empiri

vil belyse sentrale aspekter ved hvordan russisk helhetlig tilnærming og maritim doktrine kan gi oss utfordringer med å opprettholde en tilstrekkelig situasjonsforståelse i det maritime domenet. Primærkildene her er offentlige dokumenter, mens sekundærkildene består av artikler, bøker og andre studier på tematikken. Den kvalitative analysen vil slik nyansere bildet og funnene i analysedelen.

Oppgavens analysedel fokuserer på hvordan kartlegging av maritime nettverk bestående av fartøy, selskaper og områder kan bidra til økt situasjonsbevissthet. Analysedelen vil gjennomføres for å illustrere den merverdi bruk av stordata og SNA kan gi oss. Analyseverktøyene som er videreutviklet og benyttet i forbindelse med studien er R og Rstudio. R er et objektorientert programmeringsspråk, mens Rstudio er et integrert utviklingsmiljø for statistisk databehandling og grafikk. Dette vil bli nærmere beskrevet i kapittel syv.

Studien er ugradert. Dette medfører en viss begrensning på omfanget av data som blir presentert. Studien tilkjennegir allikevel russiske fartøyer som vurderes å avvike fra det man forventer i en normalsituasjon. Gjennom analyser av åpne kilder vil også eierstruktur bli tilkjennegitt, og nettverkspresentasjoner vil bli gjort både mellom fartøy, eierstrukturer og geografiske områder. Hendelser i tidsperioden, som militære øvelser, vil bli brukt som eksempler som vil kunne motivere russiske myndigheter til å endre adferd, ved å bruke tilgjengelige virkemidler til sin fordel.

# 2.1 Datainnsamling

## Intervju med tidligere Forsvarssjef General Sverre Diesen

Pensjonert general og tidligere Forsvarssjef Sverre Diesen er i dag ansatt ved Forsvarets Forskningsinstitutt (FFI). Hans tyngde og erfaring fra forsvarssektoren samt hans nylig utgitte rapport «Lavintensivt hybridangrep på Norge i en fremtidig konflikt» var et viktig bidrag for å få en generell oversikt over hybridbegrepet og begrepets relevans i dag. Intervjuet ble gjennomført onsdag 10. oktober 2018, og hensikten var å knytte hans erfaringer og synspunkter på hybrid krigføring til denne studiens problemstilling. Intervjuet ble gjennomført som en diskusjon rundt begrepsbruk og utfordringer med hybride trusler i norske interesseområder.

## Korrespondanse med Admiral James Stavridis

Admiral James Stavridis er pensjonert firestjerners admiral fra U.S Navy som blant annet tjenestegjorde som den 16. Supreme Allied Commander Europe (SACEUR). Kommunikasjonen med admiralen foregikk på mail i forbindelse med arbeidet på Naval Postgraduate School (se under). Stavridis har skrevet en rekke bøker og artikler om blant annet sikkerhetspolitikk og sjømakt. Hans artikkel «Maritime Hybrid Warfare is Coming» som er brukt som referanse i

denne studien tegner et skremmende bilde av maritim hybrid krigføring (Stavridis, 2016). Henvendelsen til Admiral Stavridis gjaldt hans syn på om det kan være et sammenligningsgrunnlag mellom aktiviteten han beskriver i Sør-Kina-havet og til russisk aktivitet i nordområdene og Baltikum. Stavridis har gitt sin forhåndsgodkjenning til at hans tilsvar (i sin helhet gjengitt i kapittel 2) kunne inkluderes i denne studien.

## Forsvarets Operative Hovedkvarter (FOH)

Datainnsamling fra FOH besto av samtaler og observasjoner for hvordan maritim situasjonsforståelse på operasjonelt nivå skapes. Fokuset for samarbeidet med FOH var å kartlegge hvilke aktører, prosesser, resultater og hvordan distribusjonskanaler for maritim situasjonsforståelse fungerer i dag. Samarbeidet med FOH danner rammeverket for kapittel tre i denne oppgaven.

## AIS stordata

Kystverkets databaser ble brukt for å hente ut AIS data for perioden 2014 og 2017. Datagrunnlaget i innsamlede AIS data for 2014 utgjør nærmere 25 millioner rader med statistiske data for hver måned, kun for russiske fartøy. Etter 1. januar 2015 ble også AIS satellittdata lagret av Kystverket. Dette gjør at størrelsen på datasettet øker fra 2014 til 2017. Størrelsen på datasettet fra 2017 rundt 5 terrabytes. For alle skip fra alle nasjonaliteter i settet utgjør dette 20 millioner rader data per dag. Formatet på datasettet var kompatibelt med analyseverktøyene anvendt i denne studien. Hensikten er at gjennom integrering og manipulering av AIS data er det gjennom analytisk tilnærming mulig å sannsynliggjøre tilhørighet i mørke eller grå maritime nettverk.

## Erfaringsutveksling og utvikling av analyseverktøy ved Naval Postgraduate School, Monterey, California.

I perioden 16.- 21. september 2018 ble det i forbindelse med oppgaven gjennomført et besøk til Naval Postgraduate School (NPS) i Monterey, California. Reisen ble gjennomført sammen med bi-veileder og sjefsforsker ved FFI, Frank B. Steder. Hensikten var erfaringsutveksling med teamet bak studien «Mapping Dark Maritime Networks» som i april 2018 kunngjorde sin studie hvor SNA ble benyttet til kartlegging av kinesiske maritime nettverk involvert i oppbygging av kunstige øyer i Sør-Kina-havet. Denne studien vil bli redegjort for i kapittel seks[2]. Littoral Operations Center ved NPS og analyseavdelingen CORE lab, bidro for å videreutvikle analyseverktøyene benyttet i denne forskningen. Formålet med dette var å tilpasse koder og algoritmer for kartlegging av potensielle maritime hybride trusler i norske interesseområder.

[2] Se pkt 6.2

## 2.2 Reliabilitet, validitet og generaliserbarhet

### Reliabilitet

Reliabilitet er knyttet til målekvalitet, kvaliteten på målingene og om vi kan stole på dataene som er kartlagt (Busch, 2013, s. 62). Reliabiliteten kan altså si oss noe om innsamling av data er gjort på en pålitelig måte, og om en re-test av datagrunnlaget hadde gitt høy grad av korrelasjon (Creswell, 2014, s. 247). Datasettet som er analysert i studien er datert 2014. Som tidligere nevnt i oppgaven startet Kystverket implementering av AIS satellitt-data registreringer i 2015. Den teknologiske utviklingen av AIS datainnsamling gjør at datasettet for 2017 inneholder mange flere registrerte datapunkter, og dermed blir datasettet større (flere rader). Vi kan ikke utelukke at dette vil påvirke datagrunnlaget og dermed resultatet av analysen. Sosiale nettverk er dynamiske og endres oftere i motsetning til mer stabile variabler som måler egenskaper (for eksempel kjønn). Oppgaven tar for seg analyse av både kvalitative og kvantitative data. Etterprøvbarhet vil være mulig gitt samme AIS-datasett og analyseverktøy som beskrevet i kapittel syv, hvor jeg har forsøkt å gjøre prosessen så transparent som mulig ved å beskrive modellering på en detaljert måte. Analytikere ved NPS, FFI og meg som masterstudent har behandlet det kvantitative datasettet. De litterære kildene i den kvalitative delen av oppgaven vil også kunne etterprøves.

### Validitet

Validitet eller gyldighet forteller oss noe om man kan trekke relevante og meningsfulle slutninger fra undersøkelsen (Creswell, 2014, s. 250). Validiteten forteller oss i hvor stor grad benyttede data er gyldige for problemstillingen studien tar for seg (Busch, 2013, s. 62). Måles det man tror man måler? Tilnærmingen til oppgavens problemstilling er todelt. Først benyttes en kvalitativ analyse av russisk helhetlig tilnærming til konflikt fokusert på russisk maritim doktrine. Deretter utvikles verktøy som anvender metoder fra SNA for å undersøke om nettverksanalyse kan gi oss en økt maritim situasjonsbevissthet. Dette vil muliggjøre nærmere undersøkelser av det komplekse bildet av maritime nettverk som opererer i våre interesseområder. Videre vil det være mulig å vise til metoder for å gjennomføre statistiske analyser av mulige nettverk som utøvere av en russisk tilnærming til konflikt, herunder russisk maritim doktrine. Å anvende flere perspektiver eller teorier til å tolke data kalles triangulering og benyttes i den hensikt å undersøke funn fra ulike kilder, som kan styrke validiteten i en studie (Creswell, 2014, s. 201).

### Generaliserbarhet

Generaliserbarhet er knyttet til om resultatene er overførbare og relevante i andre sammenhenger enn de som er studert (Busch, 2013, s. 62). I denne studien er kvalitative data benyttet for å

studere sammenhenger i det komplekse bildet de kvantitative dataene representerer. Hensikten med analysen vil ikke være å generalisere, men å gi dypere innsikt i problemstilling og øvrig tematikk for å danne grunnlag for videre forskning og videre utvikling i norsk maritim sektor.

## 2.3 Etiske vurderinger

Da analysen åpner mulighet for å identifisere enkeltfartøyer og deres eierstruktur ble prosjektet meldt inn til personvernombudet for forskning ved Norsk Senter for Forskningsdata (NSD). Godkjenning av prosjektet ble mottatt av personvernombudet før analysen ble gjennomført. Ifølge prosjektmeldingen skal eventuelle innsamlede opplysninger anonymiseres ved prosjektslutt 26.november 2018. Grunnet studiens etiske standpunkt i forhold til personvern samt graderingsnivået på oppgaven vil personer knyttet til drift av de ulike maritime nettverkene ikke bli identifisert dersom dette ikke allerede er tilkjennegjort i andre studier, eller gjennom media. Anonymisering innebærer å bearbeide datamaterialet slik at ingen enkeltpersoner kan gjenkjennes[3]. Det gjøres ved å:

- slette direkte personopplysninger (som navn/koblingsnøkkel)
- slette/omskrive indirekte personopplysninger (identifiserende sammenstilling av bakgrunnsopplysninger som f.eks. bosted/arbeidssted, alder og kjønn

Oppgavens har som ambisjon å øke evne til kartlegging av hybride trusler og fokuserer således på et alvorlig tema med potensielle alvorlige konsekvenser. Å omtale russiske sivile fartøyer og selskaper i en slik studie er utfordrende. Det er ikke oppgavens hensikt å rette mistanke mot enkeltfartøyer, deres besetninger eller eiere. Normal seilas og virksomhet tolkes derfor ikke som å være noe annet, til tross for at dette kommer frem i datagrunnlaget. Basert på sin adferd har enkelte av disse blitt fanget opp av det filter og den koding som er satt i analyseverktøyene. Eksemplene som presenteres i oppgavens analysedel utgjør et fåtall av analysens totale resultater, men blir benyttet der det eksisterer mønster og sammenhenger som er relevante i lys av oppgavens problemstilling.

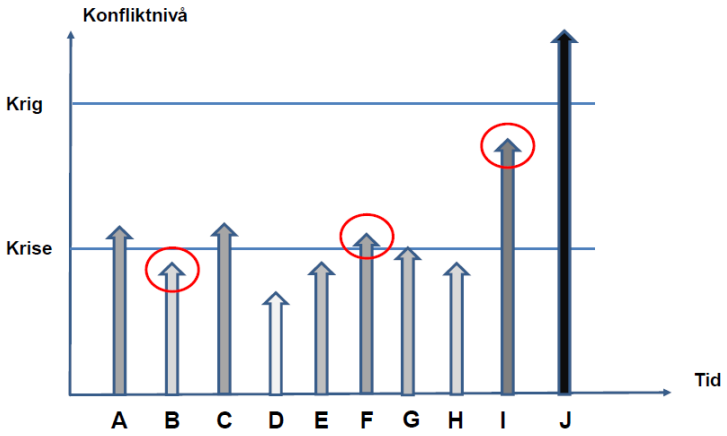
[3] Se vedlegg A

# 3 Russisk «helhetlig tilnærming»

Hybridbegrepet er omdiskutert, og en allmenngyldig felles definisjon eksisterer ikke. Er maritime hybride trusler i våre interesseområder en reell utfordring? Dette kapittelet vil beskrive hva som omfattes av begrepet, diskutere hvorvidt dette er dekkende for russisk tilnærming til konflikt, og deretter knytte dette til russisk maritim doktrine. Robert Seely refererer til Basil Liddell Harts bok *Strategy,* utgitt i 1954: *«...the use of all the levels of state power – is a terra incognita – still awaiting exploration and understanding..» (Seely, 2017)*

Det har blitt gjort en rekke forsøk på å sette merkelapp på det russiske konseptet for tilnærming til konflikt. Før den videre analysen er det derfor oppgavens hensikt å rydde i begrepsapparatet for å forstå hva litteraturen sier om denne tilnærmingen. Intervjuet med General(p) Sverre Diesen onsdag 10. oktober brukes her som en innledning. Diesens betraktninger:

> *Russisk strategi og doktrine må ses i sammenheng med den tilnærmingen de revisjonistiske stormaktene Russland og Kina har inntatt som en konsekvens av amerikansk overlegenhet med hensyn til konvensjonell militærmakt. Hybridkrigføringens fokus på økt bruk av irregulære virkemidler til fordel for konvensjonelle maktmidler gjør at påvirkning av motpartens vilje og situasjonsforståelse i noen grad erstatter maktanvendelse av fysisk karakter. Denne formen for krigføring gjør at det kan bli utfordrende å fastslå om det pågår angrep eller ikke, samt at det også er utfordrende å slå fast hvem som står bak, avhengig av om hendelsene er attribuerbare eller ikke-attribuerbare. Uvisshet rundt dette kan medføre at det skapes tilstrekkelig usikkerhet hos den som utsettes for dette til at for eksempel NATOs artikkel 5 kan tre i kraft. Norske myndigheters evne til å håndtere en slik situasjon, ta kontroll på narrativet, og beskytte innbyggerne kan bli utfordret. Dersom Norge blir utsatt må vi kunne skape en situasjon som vil trigge alliert støtte. Når det kommer til anvendelse av hybridkrigføring sett fra Russlands side er Vestens tilnærming til land som tidligere var en del av Sovjetunionen, eksempelvis Ukraina, en innblanding i russiske anliggender. Fra et russisk ståsted er det Vesten som beviselig har drevet hybrid krigføring mot Russland. Strategien fra en angriperstat i en innledende fase vil være å skjule faktiske hybride tiltak for en motstander ved å tilstrebe at de fremstår som tilfeldige, uskyldige hendelser.*




Figur 3.1 «Hendelser med hybridkrigføringskarakter»

Figur 3.1 er hentet i fra Sverre Diesens FFI rapport *«Lavintensitets hybridangrep på Norge»* og illustrerer disse betraktningene. Irregulære virkemidler kan innrettes slik at de skjules blant uskyldige hendelser. Hendelse B, F og I er hendelser med hybrid karakter. De øvrige er uskyldige, tilfeldige eller iscenesatte. Dette gir mulighet for å eskalere en konflikt horisontalt, uten å øke intensiteten og dermed krysse grensen for det som utløser NATOs artikkel 5 (Diesen, 2018, s. 22). Oppgavens utgangspunkt er at russiske maritime nettverk i norske interesseområder kan representeres ved en slik hendelse, der det først i ettertid vil være mulig å se hvordan disse passet inn i et større mønster.

Hurtigheten og besluttsomheten i operasjonene på Krim gjorde at Vesten satt famlende igjen og lette etter måter å respondere på (Giles, 2016, s. 4). Det *hybride* lå i Russlands kombinerte bruk av militære, diplomatiske og økonomiske virkemidler for å undergrave NATO og alliansens partnere (Lasconjarias & Larsen, 2015, s. 116). Hybrid krigføring er designet for å utnytte nasjonale sårbarheter i hele spekteret fra politisk, militært, økonomisk, det sosiale, informasjonsmessige og infrastrukturmessige (PMESII) (Cullen & Reichborn-Kjennerud, 2017, s. 4). Gjennom koordinert bruk av statens militære, politiske, økonomiske, sivile og informasjonsmessige maktmidler (MPECI) søker en hybrid aktør å oppnå effekt som overstiger virkningen av militære virkemidler (Cullen & Reichborn-Kjennerud, 2017, s. 4). Effekten av synkroniseringen av effekter avhenger av tilgjengelige midler og de oppfattede sårbarhetene hos en motstander (Cullen & Reichborn-Kjennerud, 2017, s. 9). Diesen viser til attribuerbare og ikke-attribuerbare hybride trusler i intervjuet og disse er gjengitt i figur 3.2. Disse kan knyttes til MPECI, og gi seg utslag i både kinetiske og ikke-kinetiske operasjoner gjennom synkroniserte angreps pakker (Synchronized attack packages – SAP) som er skreddersydd og tilpasset svakheter i det system de er ment å virke, og som ideelt sett er under terskelen for å bli detektert

som et hybridangrep (Cullen & Reichborn-Kjennerud, 2017, s. 9). Mørke og grå maritime nettverk kan i ytterste konsekvens ha en funksjon i hele dette spekteret, men størst relevans i denne oppgaven har allikevel kinetisk/ikke-attribuerbare operasjoner.

| | **Kinetisk** | **Ikke-kinetisk** |
|---|---|---|
| **Attribuerbar** | Kinetiske og attribuerbare småoperasjoner som ikke primært skal realisere regulære militære mål (ta lende, slå fienden, ødelegge bestemte militære kapasiteter), men understøtte eller styrke kredibiliteten til et strategisk narrativ[30] («Vi ønsker å fremme fred og demokrati», «Vi er kommet for å frigjøre dere» etc.). | Åpenlyse informasjons- eller påvirkningsoperasjoner som skal bearbeide holdninger og adferd hos målgruppen gjennom kanaler som statskontrollerte medier, informasjonskampanjer i statlig regi etc. |
| **Ikke-attribuerbar** | Fordekte kinetiske operasjoner som sabotasje, attentater, bombeangrep o. l., utført av spesialstyrker uten uniformer eller kjennetegn, eller av stedfortredere som militser, opprørsgrupper, «selvforsvars-organisasjoner» mv. | Manipulering av nyhetsbildet og andre fordekte påvirkningsoperasjoner gjennom alle typer medier og plattformer, cyberoperasjoner rettet mot samfunnsviktig infrastruktur, utløsning av demonstrasjoner og annen utnyttelse av ikke-voldelige sympatisørgrupper. |

Figur 3.2 Diesens kategorisering av irregulære operasjoner (Diesen, 2018, s. 16)

NATOs helhetlige tilnærming, *Comprehensive Approach* (CA), innebærer at operasjoner gjennomføres med hensyn til hele spekteret av PMESII, og at planlegging og gjennomføring ivaretar alle disse faktorene for å oppnå en ønsket sluttsituasjon i et konfliktområde. Seely understreker dette ved å peke på at også russiske myndigheter ser på den effektive orkestreringen av alle statens virkemidler som kritisk for å oppnå ønsket effekt (Seely, 2017, s. 55). Er den russiske reaksjonen på dette blitt en «*mørk refleksjon av NATOs helhetlige tilnærming*», slik NATOs generalsekretær Jens Stoltenberg uttalte i åpningstalen til NATOs Transformation Seminar i mars 2015 (NATO, 2015)?

# 3.1 Mot en offensiv «helhetlig tilnærming»?

Den russiske opptredenen mot Ukraina tidlig i 2014 skapte med sin distinkte tilnærming grobunn for å anta at vi var vitne til en fundamentalt ny tilnærming til konflikt. De sammensatte virkemidlene ble kombinert på uforutsette måter, og har skapt debatt i ulike fagmiljøer. Som Michael Kofman beskriver det i artikkelen «Russian Warfare and other Dark Arts», blir hybridbegrepet nå brukt om all aktivitet som kan spores til Russland, og alt som favnes av virkemidler fra propaganda til konvensjonell krigføring (Kofman, 2016). Før oppgaven beveger seg videre inn i det maritime domenet for å analysere om russisk helhetlig tilnærming og maritime hybride trusler utgjør en reell utfordring for oss, har denne delen av oppgaven først til

hensikt å etablere et felles utgangspunkt for forståelsen av konseptet. Derfor vil det i dette avsnittet bli gitt en begrunnelse for hvorfor studien også omtaler det anvendte begrepet *hybrid krigføring* som *russisk helhetlig tilnærming*. Mange lesere vil sikkert finne dette overflødig ettersom hybridbegrepet er i ferd med å feste seg som en etablert beskrivelse av den «nye» formen for krigføring. Det er nettopp grunnet kontroversen som hersker rundt begrepsbruken at denne diskusjonen er nødvendig.

Charles K. Bartles beskriver russisk tilnærming til konflikt som «a new way of warfare that blends conventional and unconventional warfare with aspects of national power» (Bartles, 2016, s. 30). I denne oppgaven tolker jeg konseptet ut i fra Sverre Diesens nyansering av begrepet hybrid krigføring, nemlig som summen av virkemidler, konvensjonelle (regulære) og ukonvensjonelle (ikke regulære), russiske statlige og ikke-statlige aktører bruker for å oppnå strategiske målsetninger (Diesen, 2018, s. 10). Hybrid krigføring er altså sagt på en annen måte «en rekke militære og ikke militære handlinger som havner i gråsonen mellom åpenbar krig og dyp fred» (Hicks, 2018, s. 5). Som tidligere Supreme Allied Commander Europe (SACEUR), Admiral James Stavridis, påpeker er den fundamentale tanken bak hybrid krigføring å finne et handlingsrom i gråsonen for å skape taktisk, operasjonell og strategisk virkning. Hvis tilstrekkelig tvetydighet kan skapes tjener dette den hybride aktørens muligheter til å oppnå sine målsettinger uten å bruke åpne konvensjonelle virkemidler (Stavridis, 2016). Russland vil slik kunne holde seg under terskelen for å utløse NATOs artikkel 5. I tillegg har denne formen for krigføring til hensikt å minimere risiko for konvensjonell krig (Johnson, 2018, s. 158). En rekke kretser hevder at Moskva har utviklet hybrid krigføring som doktrine og operasjonell strategi (McDermott, 2016, s. 97). Den provoserende og destabiliserende adferden har ført til et økt behov for å overvåke og forstå den russiske aktiviteten (Hicks, 2018, s. IV). Hybrid krigføring som begrep har blitt revitalisert i en rekke fagkretser, og er i dag i ferd med å bli en modell for det som kjennetegner russisk tilnærming til konflikt i nåtid, og i analyser for hva som inngår i konseptet i fremtiden. Men som Hall Gardner påpeker i «NATO's response to hybrid threats», skyldes mangelen på en klar definisjon at begrepet forsøker å definere en flerdimensjonal tilnærming til konflikt ment for en rekke ulike formål (Lasconjarias & Larsen, 2015, s. 164).

Keir Giles kritiserer også hybrid-begrepet. Han hevder dette ble skapt av et behov for å konseptualisere og forstå en tilnærming til konflikt som ved første øyekast virker ny og fremmed, men som egentlig har røtter tilbake til Sovjettiden (Giles, 2016, s. 2). Bartles støtter dette synet, og trekker således klare paralleller mellom NATOs operasjoner i det tidligere Jugoslavia og opprettelsen av Kosovo som egen stat og den russiske annekteringen av Krim, for

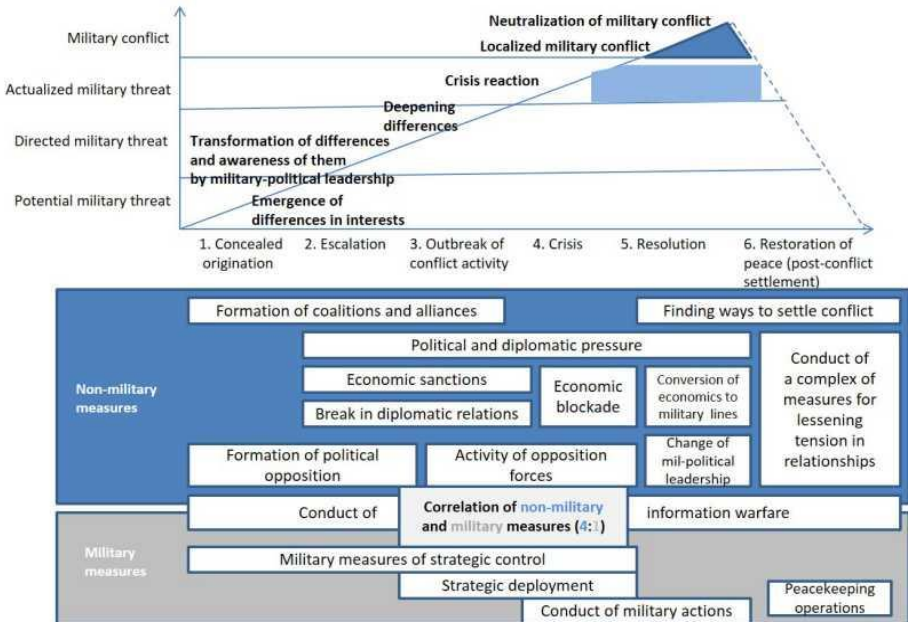
å forklare at den «hybride krigføringen» ikke representerer noe nytt og unikt (Bartles, 2016, s. 32). McDermott hevder at det er de politiske, økonomiske, kulturelle, historiske, og egenskapene ved statsapparatet i Ukraina som formet operasjonene under Krim-krisen. Han hevder at Russland designet operasjonene etter operasjonelle behov heller enn å basere dem på en modell (McDermott, 2016, s. 103). Robert Seely går enda lenger i sin kritikk av hybridbegrepet. I artikkelen «Defining Contemporary Russian Warfare» viser han til Ruslan Phukovs avvisning av begrepet. Phukov hevder at handlingene på Krim og i Ukraina representerer ingrediensene i en hvilken som helst lavintensitetskonflikt de siste århundrene, og at integrasjon av militære og ikke-militære virkemidler er brukt som «et alfabet i hvilken som helst krig siden antikken». Seely hevder at Phukov representerer samme syn som mange russiske skribenter, og hevder man kan tolke dette synet som en indirekte kritikk av Vestens manglende integrasjon av militære og ikke-militære virkemidler som igjen har ført til en økt avhengighet av teknologi, selv i konflikter der sivilbefolkningen er kritisk for å oppnå suksess (Seely, 2017, s. 52). Ser man begrepsbruken i lys av dette, kan det hevdes at den russiske tilnærmingen enten ved bruk av åpne eller skjulte virkemidler, direkte eller indirekte, med militære eller ikke-militære virkemidler er en variant av det standpunkt NATO selv tok da for første gang introduserte begrepet Comprehensive Approach under toppmøtet i Riga 2006 (NATO, 2006). Seely hevder at selv om den russiske tilnærmingen lett kan bli tolket som noe nytt, har virkemidlene vært brukt tidligere også av blant annet UK og USA. Forskjellen ligger, mener han, i den mer helhetlige tilnærmingen vi ser fra russisk side (Seely, 2017, s. 52).

Mark Galeotti hevder i artikkelen «Hybrid, ambiguous, and non-linear? How new is Russia's «new way of war?» at konflikten i Ukraina har sentrale likhetstrekk med tidligere konflikter i både Syria, Afghanistan og Irak. Galeotti hevder at det som skiller situasjonen i dag kontra tidligere konflikter er konteksten disse utspiller seg i. Han kaller dagens tilnærming «gerilja geopolitikk» utøvd av en nasjon som er klar over at dens ambisjoner overgår sine militære ressurser, og derfor må bruke andre metoder for å oppnå sine mål (Galeotti, 2016, s. 283). Ifølge Galeotti var en viktig bidragsyter i operasjonen på Krim i 2014 de paramilitære «lokale frivillige» som det i ettertid har vist seg var aktører involvert organisert kriminalitet som ikke bare utgjør en viktig maktfaktor på halvøya, men som også har tette forbindelser til russiske interesser og til forretningsmannen og politikeren Sergei Aksenov, som ble innsatt som provisorisk regjeringssjef på Krim den 27. februar (Galeotti, 2016, s. 284-285). Som litteraturen viser er spekteret av virkemidler ikke nye, men anvendelsen av irregulære og konvensjonelle virkemidler har i lys av de senere års hendelser og sikkerhetspolitiske utvikling blitt mer sømløs. Russland kan tilsynelatende ha kommet over den doktrinelle, og intellektuelle barrieren mellom

regulære og irregulære tiltak, og andre statlige virkemidler som diplomati (Seely, 2017, s. 56). Hvordan er dette overførbart til det maritime domenet?

## 3.2 Russisk maritim doktrine

General Valery Gerasimov, sjefen for den russiske generalstaben, har ifølge Lasconjaras og Larsen registrert en fundamental endring i krigens karakter der graden av politiske, diplomatiske og økonomiske ikke-militære virkemidler satt i sammenheng med militære virkemidler er 4:1 (Lasconjarias & Larsen, 2015, s. 148). Charles K. Bartles trekker også dette frem som en av de mest interessante aspektene ved artikkelen, som den russiske generalen publiserte i Voyenno-Promushlennyy Kurier (VPK), 26. februar 2013 (Bartles, 2016, s. 34). Artikkelen er siden blitt kjent som «Gerasimov-doktrinen».




Figur 3.3 «Gerasimov doktrinen» – russisk forståelse av moderne krigføring (Bartles, 2016, s. 35).

I artikkelen «Hybrid, ambiguous and non-linear: How new is Russias new way of war» tolker Mark Galeotti Gerasimovs artikkel til å beskrive en militærfaglig retning hvor viktigheten av ikke-militære virkemidler for å oppnå politiske og strategiske mål har økt og i mange tilfeller overgår bruk av militære våpen i effektivitet (Galeotti, 2016, s. 289). Metodikk og fokus i konflikter har endret seg mot en helhetlig tilnærming som inkluderer utstrakt bruk av politiske, økonomiske, informasjonsbaserte, og andre ikke-militære virkemidler sammen med motstandsgrupper i befolkningen. Disse virkemidlene sammen med bruk av militære virkemidler av en fordekt karakter, inkludert informasjonsoperasjoner og spesialstyrkeoperasjoner, utgjør nå

de sentrale elementer i en konflikt (Galeotti, 2016, s. 286). Kritiske røster har stilt spørsmålstegn ved det vestlige begrepet hybrid krigføring, og hevder at Gerasimovs artikkel har blitt brukt som en «hellig gral» for å forstå den russiske bruken av hard og myk makt, og at vestlige analyser har fullstendig forvandlet artikkelen fra å diskutere russisk persepsjon av trusselbildet, til å forklare russisk adopsjon av hybrid krigføring som et nytt verktøy for staten (McDermott, 2016, s. 99). Diesen påpeker i den forbindelse at Gerasimov mener Vesten er de egentlige foregangsland for hybridkrigføring. Eksemplene fra revolusjonene i Georgia og Ukraina fremstår sett fra russisk side som vellykkede eksempler på vestlig hybridkrigføring (Diesen, 2018, s. 9).

Som direktør ved Russia Maritime Studies Institute ved United Stated Naval War College, Michael B. Petersen hevder, er den russiske maritime doktrinen fra 2015, en av de viktigste doktrinelle uttrykk på mange år (Davis, 2015, s. 2). Dokumentet definerer russisk statlig policy hva angår maritime aktiviteter for å sikre en bærekraftig utvikling og nasjonal sikkerhet for Russland (Davis, 2015, s. 5). Doktrinen er en oppdatert oversikt over Russlands målsettinger i det maritime domenet. Dokumentet byr på første gang siden forrige versjon ble publisert i 2001, en rik innsikt i hvordan Russland ser på maritim aktivitet i dag, og hvordan ambisjonene for den maritime sektoren er i fremtiden (Connolly, 2017, s. 2). Dokumentet blir ansett som en kontinuitet fremfor et brudd med tidligere russisk doktrinell tilnærming til det maritime domenet. Det som skiller 2015 versjonen fra tidligere doktriner er fokuset på både Nord-Atlanteren og Arktis som en respons på NATOs aktiviteter, samt kampen om naturressursene der (Sergunin & Konyshev, 2017, s. 175). Doktrinen er uansett interessant sett i lys av denne oppgaven ved at den bekrefter en russisk helhetlig tilnærming også i det maritime domenet. Etableringen av «Marinestyret» *(morskaya kollegiya)* ble gjort for å koordinere strategisk planlegging for gjennomføring av doktrinen. Styret har medlemmer fra både styresmakter og rådgivere fra industrien (Connolly, 2017, s. 6). I utdraget fra «Principles of the National Maritime Policy» står det:

> ***8. The following guidelines are principles of the National Maritime Policy that govern the subjects of National Maritime Policy during its development and implementation:***
>
> ***8 d*** *«A comprehensive approach to maritime activity and its differentiation in certain areas, taking into consideration the changes in priorities depending on the volatile geopolitical situation;» (Davis, 2015, s. 8)*
>
> ***8 f*** *«Cooperation and coordination of efforts between federal entities of state power, government organizations of the subjects of the Russian federation, local governments, and public interest groups in development and implementation of the National Maritime Policy;» (Davis, 2015, s. 8)*

> ***8 k*** *«Effective state control and oversight of the vessels sailing under the state flag of the Russian Federation on the World Ocean, including state control over ports and control over the condition and use of the natural resources in the internal waters, territorial seas, exclusive economic zone, and continental shelf of the Russian Federation;» (Davis, 2015, s. 8)*
>
> ***8 l*** *«Focusing efforts on the building and development of Russian Fleet infrastructure on the territories of the subjects of the Russian Federation, traditionally connected to the maritime activities, and designating the infrastructure for military, scientific, or economic needs;»(Davis, 2015, s. 8)*
>
> ***8 m*** *«Support the Russian Navy in readiness to accomplish missions, as well as the mobilization of marine transport, fishing vessels, scientific research, and other specialized fleets and organizations to support their activities;» (Davis, 2015, s. 8)*
>
> ***8 n*** *«Systematic naval training of the vessels' crew, leadership of the shipping companies, and state government branches to operate in war time;» (Davis, 2015, s. 9)*

I tråd med Gerasimovs synspunkter på viktigheten av ikke-militære virkemidler i dagens konflikter fremhever doktrinen viktigheten av integrasjon mellom sivile og militære aktører under statlig kontroll for å oppnå strategiske ambisjoner. Bruk av sivile fartøyer for å oppnå strategiske målsettinger mot et NATO-medlem som Norge kan være velegnet for å ikke utløse artikkel 5. Russisk helhetlig tilnærming har ifølge Mark Galeotti oppstått som en respons på et dilemma der nasjonen har søkt å fremstå så mektig og imperialistisk som mulig til tross for begrensede ressurser (Galeotti, 2016, s. 296). Russisk maritim doktrine anerkjenner i lys av dette både russiske militære og sivile fartøyer som en viktig bidragsyter til russiske myndigheters projeksjon av sjømakt. Følgende viktige faktorer er viktige å ta med seg i denne sammenheng: (Galeotti, 2016, s. 291-292):

1. Villigheten til å gi ikke-kinetiske operasjoner, størst plass.
2. Den tette institusjonaliserte forbindelsen med, og bruk av ikke-statlige aktører, selv dem uten åpenbare tilknytninger til Russland.
3. En enhetlig kommandostruktur som i stor grad knytter sammen politiske og militære operasjoner.

Hvis man ser på Galeottis faktor 2 og 3 over og knytter dette til russisk maritim doktrine og studien «The Odessa Network» der våpeneksport fra Russland og Ukraina gjennom Odessa knyttet russiske statlige aktører opp mot kriminelle nettverk på Krim, er det nærliggende å trekke koblinger mellom det å bruke organisert kriminalitet på land under annekteringen av Krim til andre deler av det maritime domenet (Wallace & Mesko, 2013). I våre nærområder er sårbarheten stor og mulighetene mange.

## 3.3 Sårbarheter i norske interesseområder

Den russiske styrkeoppbyggingen og deres tilnærming til konflikt skaper utfordringer for oss, og gjør oss mer sårbar. Langtrekkende presisjonsvåpen, og kapasiteter innen cyberoperasjoner samt fordekt bruk av militærmakt er skissert som eksempler på de åpenbare truslene som vil kunne påvirke oss (Forsvarsdepartementet, 2015, s. 29). Økonomisk avhengighet av inntekter fra olje og gass samt fiskeri gjør oss sårbare. Infrastruktur knyttet til olje og gass utvinning, undersjøiske rørledninger og kommunikasjonskabler er alle sårbarheter som vil ha strategiske konsekvenser skulle de bli rammet. Våre gassleveranser til kontinentet går i dag via undersjøiske rørledninger. Videre foregår 95 prosent av verdens interkontinentale kommunikasjonstrafikk som e-post, telefon, pengeoverføringer via undersjøiske kabler (Murphy, Hoffman & Schaub, 2016, s. 15). Murphy et al. trekker blant annet frem et eksempel fra Taiwan hvor 9 undersjøiske kabler ble ødelagt i forbindelse med et jordskjelv i 2006. Det tok 11 skip 49 dager å reparere, og den regionale økonomien rammes hardt. Kostnadsoverslaget fra Taiwan ble estimert til et regionalt tap på 1,5 millioner dollar per time (Murphy et al., 2016, s. 16). Forsvarsminister Frank Bakke-Jensen har uttalt at fiberkablene er en del av forsyningslinjene mellom USA og Europa som må beskyttes (NROF, 2018, s. 9). Admiral James Stavridis sin artikkel i The Huffington Post i oktober 2016 siteres også i denne sammenheng. Han advarer mot at den russiske marinen utgjør en trussel mot det undersjøiske kabelnettverket. Dette fordi det representerer etterretningsmuligheter, samt mulighet til å påføre en motstander store økonomiske belastninger (Murphy et al., 2016, s. 17).

Figur 3.4 Kommunikasjonskabler til og fra Norge[4].

Figur 3.5 Olje og gassledninger til og fra Norge.

Det maritime domenet er velegnet for bruk av en helhetlig tilnærming, hvor mulighetene for å kombinere konvensjonelle og ikke-konvensjonelle styrker og kapabiliteter er mange. Russlands tilnærming har tilført en ny dimensjon i det geopolitiske spillet. Lasconjarias og Larsen hevder at hybrid *krigføring* i seg selv ikke er noe nytt fenomen, men måten informasjonskrigføringen og manipulasjon av massemedia blir benyttet på, som vi så på Krim, representerer noe nytt (Lasconjarias & Larsen, 2015, s. 10). Det som imidlertid ikke er nytt er bruken av *maskirovka*, eller «strategisk villedning». Strategisk villedning omfatter bruk av en vidt spekter av virkemidler som har historie tilbake til sovjettiden og den kalde krigen (Jones, 2003, s. 55). Virkemidlene er utformet for å støtte politiske målsettinger samtidig som man holder seg under terskelen som vil fremprovosere uønsket eskalering eller retaliasjon (Lasconjarias & Larsen, 2015, s. 10). Dette synet deles av Michael Hofman som hevder Russland baserer sine konvensjonelle operasjoner på *maskirovka*, ved bruk av fornektelse og fordekking (Kofman, 2016).

[4] Figur 3.4 og 3.5 er generert i analyseverktøyet R, ved bruk av scriptet «Leaflet» (se kapittel 7.1)

Rapporten «Contested Seas», utgitt av Center for Strategic and International Studies (CSIS) hevder Russlands tilnærming bidrar til økt bekymring innenfor følgende tre områder: maritim hybrid krigføring, cyberkrigføring og langtrekkende presisjonsvåpen. I denne studien blir kun maritim hybrid krigføring omhandlet. Kompleksiteten i det maritime domenet kombinert med en velutviklet russisk amfibisk kapasitet gjør at bruk av hybride virkemidler er velegnet som strategi. Fordekte sivile fartøyer i kombinasjon med spesialstyrker og lett infanteri med amfibisk kapasitet gjør det mulig å manøvrere skjult i våre interesseområder (Hicks, 2018, s. IV). Slik kan mørke og grå maritime nettverk unyttes som en kinetisk-ikke attribuerbar aktør.

Forsvarets virksomhet i det komplekse maritime domenet bidrar til å sikre statens interesser på mange felt, i fred, krise og krig (Forsvaret, 2015a, s. 15). Etterrettningstrusselen fra Russland er stor, og vurderes til å ha stort skadepotensial i våre interesseområder (PST, 2018). Muligheten for at sivile fartøyer kan kamuflere militære kapasiteter og være en aktør som søker å operere i «mørket» for kunne oppnå en strategisk målsetting vil til syvende og sist ha muligheten til å påvirke situasjonsforståelsen i en slik grad at politisk handlingsrom, og evne til krisehåndtering vil kunne bli utfordret (Hicks, 2018, s. 5).

Trusselen kan også bestå av mer tradisjonelle «irregulære» kapasiteter som minekrigføring, og bruk av spesialstyrker. Rapporten fra CSIS eksemplifiserer dette med å vise til metoder og virkemidler som er grunnlag for bekymring. Bruk av russiske statseide sivile fartøyer kan tenkes å bli brukt til en rekke formål fra etterretningsvirksomhet til skjult innsetting av spesialstyrker (Hicks, 2018, s. 6). Videre er kontainerbaserte missilsystemer, som ikke kan skilles fra vanlige sivile fraktekontainere, en identifisert trussel. Dette systemet kalles Club-K og kan blant annet frakte med seg anti-overflate cruise missiler som SS-N-25 Switchblade.[5] Å lokalisere og følge slike aktører vil være svært vanskelig (Hicks, 2018, s. 5). Setter man disse kapasitetene sammen og ser de sivile fartøyene i sammenheng med spesialstyrkers evne til å operere i det skjulte, har man mulighet til å etablere nettverk av slike noder som vil kunne utgjøre en reell trussel mot maritim infrastruktur som olje og gass, undersjøiske kabler, kommunikasjonssystemer og havner. Denne trusselen vil kunne operere skjult samtidig som at slike kapasiteter eksisterer i den hensikt å tjene russiske interesser vil kunne fornektes.

I artikkelen, «Russia's tools for Confronting the West», tar Keir Giles opp et interessant tilfelle av mulige mønster det kan være utfordrende å se i sammenheng. I 2007 gjennomførte russiske militærfly en øvelse i Nordsjøen, med flygninger ut fra hangarskipet «Admiral Kuznetsov», noe som førte til at norske oljeplattformer midlertidig ble forhindret i å

[5] Hjemmesiden til Rosoboronexport: www.roe.ru/eng/catalog/naval-systems/shipborne-weapons/klab-k/

gjennomføre helikopteroperasjoner (Giles, 2016, s. 19-20). Til tross for at de russiske flyene ikke brøt noen regler, skapte dette utfordringer og Norges ambassadør til Russland leverte en formell klage (Aftenposten, 2007). I samme tidsrom skjedde det nest største oljeutslippet i Norges historie, etter at nesten 4000 kubikkmeter råolje lekket ut i samme område som «Kuznetzov» hadde operert (Giles, 2016, s. 20; Østvang & Kemp, 2007). Artikkelen antyder at det var sammenheng mellom hendelsen i Nordsjøen og russiske krigsskips forsøk på å hindre fartøyer fra å legge kraft- og telekommunikasjonsledninger mellom Sverige og Litauen åtte år senere (Giles, 2016, s. 20).

Ser vi til andre irregulære virkemidler i det maritime domenet tegner James Stavridis et skremmende bilde i sin artikkel «Maritime Hybrid Warfare is coming». I artikkelen knytter han de hybride virkemidlene til det maritime domenet. Han hevder at i stedet for å bruke identifiserbare «gråmalte» marinefartøyer, vil trusselen i det maritime domenet bestå av en rekke sivile fartøyer fra handelsfartøyer til fiskefartøyer samt mindre hurtiggående båter. Stavridis fremhever at slike maritime fordekte virkemidler også sannsynligvis vil kunne inneha en kommando og kontrollstruktur, og potensielt bli ledet fra eksempelvis kystvaktfartøyer. Artikkelen trekker frem at dette allerede er et innarbeidet konsept i både Kina og Iran, og at disse nasjonene bruker sin kystvakt (og revolusjonærgarden i Iran) i henholdsvis Sør-Kina-havet og den arabiske gulfen. I stedet for «små grønne menn» er fartøyene som inngår i slike nettverk bemannet av «små blå (sjø)menn», militært personell som ikke er uniformerte. Dette gjøres for å muliggjøre operasjoner uten å bli knyttet opp mot en statlig aktør, som er en potensiell trussel mot sårbare interesser. Videre er infrastruktur, som undersjøiske kabler, og rørledninger i tilknytning til off-shore-næringen spesielt utsatt for denne type angrep (Stavridis, 2016). Trusselen mot olje og gass installasjoner og tilhørende systemer synliggjøres også i rapporten «Hybrid Maritime Warfare and the Baltic Sea Region» av Hoffman, Murphy og Schaub. Rapporten fremhever økonomiske sårbarheter i form av olje og gass installasjoner, og rørledninger knyttet til disse som hovedmål for maritime hybride trusler i regionen (Murphy et al., 2016, s. 28). Disse synspunktene støttes av Andrew Erickson i artikkelen «America`s security role in the South China Sea». Her peker han på Kinas maritime milits som en fremskutt trussel og del av en strategi som utfordrer USA i å bruke militærmakt mot ikke-militært personell (Erickson, 2016, s. 11). Slike elementer, hevder Stavridis, kan utgjøre en stor trussel, og blande seg med øvrig skipstrafikk fordekt av pågående fiskeri, eller langs handelsruter. Synet til Stavridis på hva som kan utgjøre en maritim trussel fremkommer også i Chris Kremidas-Courtneys artikkel «Countering Hybrid Threats in the Maritime environment». Aktører som opererer fordekt, med umerkede handels- eller fiskefartøy som kan overraske militære fartøy og

forhindre dem i å respondere på andre elementer av hybride trusler vil kunne bli en stor utfordring (Kremidas-Courtney, 2018). Samarbeid med Dr. Wayne Porter[6] ved Naval Postgraduate School i forbindelse med studien har muliggjort å få til personlig korrespondanse med Admiral Stavridis knyttet til oppgavens problemstilling. Hensikten var å undersøke hvorvidt han mener situasjonen i Sør-Kina-havet er overførbar til russisk maritim strategi. Et av spørsmålene var om hans analyse av Sør-Kina-havet har relevans i norske interesseområder. Han skriver:

> *Most of my views on the S China Sea are in the Proceedings article. In terms of transferability to Russia, I'd say pretty high overlap. They will use it in the Baltic and Black Sea, and the modalities could include maritime versions of what they are doing in Ukraine. Might be «civilian» fishing vessels, non-uniformed sailors, SPETSNATZ embarked in ships, sabotage against Ukrainian naval vessels and their growing attempts to build a new naval station in the Black Sea. In terms of the Baltic, much the same. In the North Atlantic, you could see more intelligence collection from «civilian» ships. The most interesting would be in the Arctic as the ice melts and there is an increase in shipping. (Stavridis, 2018)*

Admiral Stavridis hevder altså at erfaringer i Sør-Kina-havet er overførbare til russiske handlemåter i våre interesseområder, og at det er en økt sannsynlighet for at sivile fartøy benyttes til fordekt irregulær virksomhet, og etterretningsformål. Stavridis' synspunkter er slik sett i samsvar med de faktorer studien trekker frem fra russisk doktrine. Det maritime domenet har fått for lite fokus når det gjelder mottiltak mot trusselbildet som skisseres. At sivile fartøy kan utgjøre en hybrid trussel vil nødvendigvis påvirke vår maritime situasjonsbevissthet. I et komplekst informasjonsbilde i det maritime domenet vil det være vanskelig å skille de uskyldige hendelsene fra de irregulære virkemidlene. Mørke og grå maritime nettverk bidrar slik til å gjøre fremtidens maritime konflikter enda mer komplekse, og stiller ytterligere krav til vår evne til å skape en tidsriktig og troverdig situasjonsforståelse i det maritime domenet. Oppsummert vurderes truslene som kan utfordre vår maritime situasjonsbevissthet til å bestå av:

- Aktiviteter rettet mot maritim næring og industri med tilhørende infrastruktur, inkludert:
    - Olje og gass
    - Fiskeri
    - Undersjøiske kabler og rørledninger

[6] Sjef for «Littoral Operations Center» som er en avdeling ved Defense Analysis, Systems Engineering Departments ved Naval Postgraduate School.

- Aktiviteter der målrettet etterretningsinnhenting mot både norsk næringsvirksomhet og militær virksomhet

## 3.4 Delkonklusjon

Det eksisterer en rekke ulike definisjoner av begrepet hybrid krigføring, og man har fremdeles ikke kommet frem til en felles definisjon. Dette kapittelet har analysert sentrale utviklingstrekk og kjennetegn rundt russisk helhetlig tilnærming, og russisk maritim doktrine. Russisk tilnærming fungerer i hele spekteret fra fred til krig og omfatter koordinert bruk av alle statens virkemidler, konvensjonelle og ukonvensjonelle, hvor politiske, militære, økonomiske, sivile og informasjonsmessige tiltak settes sammen i et system. Å trekke paralleller mellom hybrid krigføring og NATOs helhetlige tilnærming er ikke ukontroversielt.

For det første har vi sett hvordan russisk helhetlig tilnærming til konflikt kan utgjøre en trussel også i det maritime domenet. Dette er et viktig moment i oppgaven fordi innsikt i utviklingstrekk i væpnede konflikters utvikling og hva som er den dimensjonerende trusselen i Norge, er grunnlaget for analysen i oppgavens andre del.

For det andre vil utviklingen av en helhetlig tilnærming i det maritime domenet, ved bruk av irregulære virkemidler til fordel for konvensjonelle maktmidler, kunne påvirke vår situasjonsforståelse. At moderne konflikter har endret karakter anerkjenes av Gerasimov, og gjenspeiles i russisk maritim doktrine. Russlands bruk av irregulære virkemidler kan gjøre det utfordrende å fastslå om det pågår angrep eller ikke. Som Diesen hevder vil det også være utfordrende å slå fast hvem som står bak, avhengig av om hendelsene er attribuerbare eller ikke-attribuerbare. Vi ser metodene brukt av Kina i Sør-Kina-havet, og dette er overførbart til våre interesseområder hvor sivile fartøyer kan bli brukt som en del av en tilnærming hvor Russland søker å oppnå sine strategiske målsettinger.

For det tredje er sårbarhetene i norske interesseområder mange, og det maritime domenet kan være en velegnet arena for hybride trusler. Bruk av fordekte virkemidler vil kunne være effektive grunnet vår strategiske plassering og våre mange næringsinteresser knyttet til det maritime domenet. *Maskirovka* i det maritime domenet er ikke nødvendigvis en ny problemstilling, men en helhetlig videreføring av konsepter vi også så i bruk under sovjet-tiden. For å kunne håndtere disse utfordringene kreves det god maritim situasjonsbevissthet.

# 4 Maritim situasjonsbevissthet i dag

Dette kapittelet gir en overordnet beskrivelse av hvordan maritim situasjonsbevissthet skapes i dag, og redegjør for aktører, prosesser og resultater innen maritim forvaltning. Kapittelet er et resultat av observasjon og samtaler med kilder ved Forsvarets Operative Hovedkvarter (FOH) gjennomført ved besøk 5. september 2018 samt litteraturgjennomgang av relevante kilder. Hensikten er å kartlegge hvordan den maritime situasjonsbevisstheten skapes i dag, og hvilke eventuelle utfordringer man ser at man har på operasjonelt nivå i Norge. Grunnet graderingsnivå vil kun hovedtrekk bli presentert.

## 4.1 Bakgrunn

Store deler av Norges økonomiske virksomhet er tilknyttet havet, og mye av vår infrastruktur for understøttelse av maritime næringer er knyttet til kystnære områder. Forsvarets oppgaver skal blant annet sikre et nasjonalt beslutningsgrunnlag gjennom overvåkning og etterretning, bidra til ivaretakelse av samfunnssikkerhet samt hevde norsk suverenitet og suverene rettigheter (Forsvarsdepartementet, 2016, s. 22). Sjef FOH utøver operativ kommando over Forsvarets styrker og han utøver sammen med sjefen for Etterretningstjenesten ansvaret for å opprettholde en god situasjonsforståelse i norske interesseområder. Sjøforsvaret skal ivareta nasjonale maritime fredsoppgaver, og samtidig være i stand til å bidra i fellesoperasjoner nasjonalt og internasjonalt. Sjøforsvaret skal kunne skape nødvendig grad av sjøkontroll og sjønektelse i både fred, krise og væpnet konflikt i utvalgte områder (Forsvarsdepartementet, 2016, s. 59).

Det maritime domenet er en viktig del av det internasjonale samfunnet, og en vesentlig del av vår samtids verdiskapning i verden er tilknyttet havet. Energiutvinning, matproduksjon og frakt av varer og tjenester er viktige ledd i den globale økonomien. Overvåkning og etterretning i disse områdene er derfor nødvendig for opprettholdelse av situasjonsbevisstheten.

«Homeland Security Presidential Directive 13» ble utgitt i 2004. Dokumentet markerer starten for bruken av begrepet Maritime Domain Awareness (MDA)[7], og beskriver et rammeverk for USAs evne til å forbedre sikkerheten i det maritime domenet. Med bakgrunn i rammeverket for MDA, ble NATOs konsept for Maritime Situational Awareness (MSA) iverksatt for å imøtekomme utfordringer med stadig økende illegal trafikk i Middelhavet. Siden den gang har utviklingen forsterket behovet for å forstå alt som kan assosieres med det maritime domenet (Hicks, 2018, s. V). I innledningen proposisjonen til siste langtidsplan, Stortingsproposisjon

[7] *«The effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of a nation or region»*

151S, er det en ambisjon fra regjeringens side å investere i fremtidsrettede, strategiske kapasiteter, for blant annet å opprettholde situasjonsforståelse og kontroll i nordområdene (Forsvarsdepartementet, 2016). Så hvordan skapes maritim situasjonsbevissthet i dag, og i hvilken grad er vi rustet til å kartlegge hybride trusler i det maritime domenet?

## 4.2 Aktører og systemer i maritim forvaltning

Forsvaret har en sentral rolle i overvåking og kontroll i det maritime domenet, og har også ressurser til rådighet for å sikre tilstedeværelse i norske interesseområder. I Forsvarets Doktrine for Maritime Operasjoner (FDMO) beskrives overvåkning og etterretning som et fundament for utøvelse av militær maritim virksomhet (Forsvaret, 2015a, s. 43). Overvåkning gjennomføres for å bygge et sanntids situasjonsbilde, mens etterretning gjennomføres for å forstå intensjoner, evner og kapasiteter i vurdering av potensielle trusler. Overvåkning og etterretning kan derfor sees på som komplementære prosesser som skal underbygge situasjonsforståelse på alle kommando-nivåer (Forsvaret, 2015a, s. 43). I norske interesseområder bidrar både nasjonale og allierte ressurser. Sjøforsvaret, med Marinen og Kystvakten, samarbeid med Luftforsvarets maritime patruljefly (MPA) og ulike allierte partnere bidrar daglig som sensorer for overvåkning av alle dimensjoner i det maritime domenet (Forsvarsstaben, 2014). Sluttnoden for den maritime situasjonsforståelsen er Forsvarets Operative Hovedkvarter (FOH) som samler både de sivile og militære bidragene. FOH bidrar til å sikre norsk evne til å etablere nasjonal og alliert situasjonsforståelse, og kan slik understøtte politiske og militære målsettinger og beslutninger i tråd med strategiske føringer.

Ansvaret for situasjonsbevissthet i det maritime domenet er delt mellom flere statlige etater, som har ansvar for å dekke sin del. Hovedaktørene i maritim forvaltning er Kystverket, Tollvesenet, Fiskeridirektoratet, Politiet, Hovedredningssentralene, og Sjøfartsdirektoratet som alle har unik kompetanse innenfor sitt ansvarsområde. Forsvarets hovedansvar er suverenitetshevdelse, Kystverket har ansvar for å tilrettelegge for sikker ferdsel og sørge for beredskap mot akutt forurensing. Grensekontroll og generell myndighetsutøvelse hviler på politiet, mens PST har ansvar for å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. Tollvesenet har kontroll av vareflyten over grensen, mens Fiskeridirektoratet har ansvar for ressurskontroll. Videre er både havnemyndigheter og den maritime næringen selv bidragsytere i overvåkningen og opprettholdelse av den maritime situasjonsforståelsen. Aktørene er mange og aktørene nevnt overfor er ikke ment å være en uttømmende liste over alle instanser som er involvert. Et innblikk i det komplekse landskapet og nettverket som bidrar til hvordan maritim situasjonsbevissthet skapes er viktig for forståelsen av kompleksiteten i prosessen.

Norske maritime myndigheter har et åpenbart behov for å integrere og sammenstille informasjon. Informasjonsdeling skjer mellom aktørene på regelmessig basis, i ulike systemer, og bidrar til å øke tverrsektorielle synergier i det maritime domenet.

## Barents Watch

Barents Watch (BW) er et prosjekt under Kystverket som utvikler tjenester for brukere med interesse i nordområdene. Her legges det til rette for informasjonsutveksling og utvikling av tjenester på tvers av de involverte etatene innenfor det maritime domenet (Blix, 2014, s. 7). Systemet skal gjøre relevant informasjon og tjenester lettere tilgjengelig for myndigheter, beslutningstakere og allmennheten (Kystverket, 2017b, s. 31). BW består av en åpen og en lukket del, der den lukkede delen ivaretar et effektivt samarbeid mellom etatene og deres behov for å utveksle informasjon. Som en del av systemets visjon er *å bidra til bedret og felles situasjonsbevissthet*, og *øke den nasjonale evnen til å detektere og forstå* aktiviteter i det maritime domenet (Blix, 2014, s. 7).

## SafeSeaNet

Dette er et såkalt «Vessel Traffic Monitoring and Information System (VTMIS) (Blix, 2014, s. 22). Systemets hensikt er å øke maritim trygghet (safety), sikkerheten for skipstrafikk til sjøs og i havneområder, beskyttelse av det marine miljøet og effektiviteten av trafikken og transporten i det maritime domenet. I norsk sammenheng er dette et elektronisk meldingssystem, administrert av Kystverket, for skip som ankommer og forlater norske havner. Sjøfartsdirektoratet, Tollvesenet, Forsvaret, Politiet, og Fiskeridirektoratet deltar i dette systemet (Blix, 2014, s. 23). Automatic Indentification System (AIS) inngår i dette systemet. AIS vil bli behandlet nærmere i kapittel fire.

Internasjonalt samarbeid er også viktig i den maritime overvåkningen. Det finnes en lang rekke med prosjekt i regi av både EU og NATO som er av relevans for maritim trygghet og sikkerhet i både Europa men også i våre interesseområder. Relevant for denne oppgaven nevnes i denne sammenheng:

## Maritime Surveillance Networking (MARSUR)

MARSUR ble startet av EU kommisjonen i 2007 som et virkemiddel for å øke samarbeid mellom alle aktører som har interesser i det maritime domenet. Norges avtale med EU ble underskrevet av Forsvarsdepartementet i 2012. Hensikten med MARSUR er å ha et europeisk nettverk for deling av maritim informasjon i nettverk og for å danne et felles operativt bilde (Recognised Maritime Picture/RMP). MARSUR er et «system av systemer» som skal bidra til en

bedre maritim situasjonsforståelse for å bedre maritim sikkerhet (safety og security), bedre interoperabilitet og samarbeid mellom medlemslandene (Blix, 2014, s. 21).

### Vessel Monitoring System (VMS)

Alle fiskefartøyer over 15 meter er pålagt å ha dette systemet ombord. Fiskefartøyenes bevegelse (posisjon, kurs og fart) registreres i tillegg til fangstrapporter. I våre interesseområder er det et avtaleregime mellom Danmark, Island, Norge, Russland og EU som gjennom North East Atlantic Fisheries Commission (NEAFC) pålegger fartøyer å rapportere aktiviteten sin (NEAFC, 2018). I Norge driftes systemet av Fiskeridirektoratet (Blix, 2014, s. 28).

## 4.3 Prosessen

Vi skiller mellom sivile og militære bidrag til prosessen rundt det å skape en best mulig situasjonsbevissthet. De sivile bidragene blir ivaretatt av aktørene omtalt i forrige avsnitt. Dette er samarbeid mellom politi, toll, losvesen, trafikksentraler, havnemyndigheter, samarbeidspartnere for grensekontroll og maritim næring. Forsvaret samarbeider spesielt tett mot Fiskeridirektoratet, Kystverket, Tollvesenet og Politiet. Prosjekter som Barents Watch og SafeSeaNet gjør det mulig for en tverrsektoriell analyse og informasjonsutveksling om forhold som har betydning for det maritime domenet. FFOD sin tilnærming til de tre nivåene som utgjør prosessen som bidrar til situasjonsbevissthet, er sammenlignbar med de tre funksjonene i MDA, beskrevet i rapporten «Contested Seas» utgitt av tenketanken CSIS (Center for Strategic and International studies) (Hicks, 2018, s. 2-3).

1. *Innhenting – er innsamling av rådata fra det maritime domenet i alle dimensjoner inkludert undervannsdomenet.* FFOD omtaler dette som situasjonsoppfattelse av observerte data (Forsvaret, 2015a, s. 133).
2. *Analyse – er evnen til å skape et enhetlig bilde for å skape dypere innsikt i det maritime domenet.* FDMO omhandler dette som å skape situasjonsforståelse - integrasjon av data og bevisstgjøring av betydningen for det som skjer (Forsvaret, 2015a, s. 133).
3. *Aktive tiltak – innhentede og analyserte data kan distribueres og gi relevant informasjon til relevante aktører for å håndtere en mulig eller eksisterende trussel.* FDMO omtaler dette som situasjonsprediksjon - en evne til å forutse hendelser basert på gjenkjenning av tidligere mønster (Forsvaret, 2015a, s. 133).

Sydd sammen med de militære bidragene fra Sjøforsvarets fartøyer, Kystvakten, kystradarkjeden, etterretning, maritime patruljefly, satelitter, og andre allierte i våre interesseområder dannes et komplekst bilde. Ved FOH settes ulike typer sensor og etterretningsinformasjon sammen til et Recognized Maritime Picture (RMP). Sammen med tilsvarende informasjon som omfattes av de andre forsvarsgrenene settes alle disse lagene med informasjon i et system og visualiseres som det som også omtales som Common Operational Picture (COP). COP er sammenstillingen av informasjonen fra alle relevante dimensjoner, presentert i ett format og bilde. Dette legger til rette for felles situasjonsbevissthet mellom nivåene i organisasjonen og representerer den overordnede situasjonsbevissthet ved FOH (Forsvarsstaben, 2014, s. 216). Det er viktig å kontekstualisere innholdet i dette for å skape forståelse. Overvåkning fra de ulike aktørene danner et integrert bilde som skaper en situasjonsbevissthet, og gjør Forsvaret i stand til å reagere og løse militære oppgaver samt yte støtte til det sivile samfunn. Truslene er mange og strekker seg fra terror til miljøkriminalitet, immigrasjon, internasjonal kriminalitet og smugling. Kompleksiteten i domenet gjør at fokuset for overvåkning og etterretning baserer seg på å kjenne normalsituasjonen over tid, se trender, og analysere potensielle avvik fra normalsituasjonen.

Hvordan man oppdager avvik i dagens situasjon avhenger av samarbeidet mellom de ulike aktørene, og om de ulike aktørene involvert i prosessen har tilstrekkelig sensordekning i de aktuelle områdene. I lys av Diesens argumentasjon i forrige kapittel, eksisterer det utfordringer med å skille uskyldige hendelser fra hendelser med hybrid karakter. Resultatet påvirkes av at bruk av skjulte og irregulære virkemidler kan gjøre det vanskelig å detektere avvik fra normalsituasjonen.

## 4.4 Resultatet

Tett integrasjon av ulike overvåkningssystemer og tverrsektorielt samarbeid gir oss i dag mulighet til å drive suverenitetshevdelse og ivaretakelse av samfunnssikkerheten. Mørke og grå maritime nettverk har som vi har sett tidligere som utgangspunkt at de ønsker å holde seg skjult. Det er verken mulig eller samfunnsøkonomisk ansvarlig å ha distribuerte sensorer i hele interesseområdet til enhver tid. Dette påvirker situasjonsbevisstheten vår, og vi har ingen garanti for at avvik vil kunne skje uten av vi registrerer det, til tross for at teknologiske fremskritt sikrer bedre og bedre sensormuligheter.

Utfordringen til NATO i dag er å rette tilstrekkelig fokus og prioritere sine begrensede ressurser mot de delene av det maritime domenet som trenger det til enhver tid (Hicks, 2018, s. 33). Dette gjelder også nasjonalt i Norge. På tross av erfarne operatører og hensiktsmessige

beslutningstøtteverktøy som BW og SafeSeaNet er informasjonsmengden stadig økende. Fra 2016 til 2017 økte den utseilte distansen for samtlige skipskategorier i norske havområder fra 43,9 millioner nautiske mil til 44,8 millioner nautiske mil. Dette utgjør en økning på rundt to prosent. Den samlede utseilte distansen i norske havområder tilsvarer i overkant av 2000 jordomseilinger rundt ekvator (Kystverket, 2018, s. 9). I møte med en slik kompleksitet i norske interesseområder finnes det i dag ingen fullverdige systemer som kan fange opp indikasjoner som i tilstrekkelig grad retter beslutningstakeres oppmerksomhet mot at noe avviker fra normalsituasjonen. Vi er blant annet i stor grad avhengig av de ulike operatørers erfaring og kompetansenivå samt den kollektive hukommelse som befinner seg i landets ulike og tallrike operasjonsrom for å sette dette i system. Det komplekse informasjonsbildet inneholder så mye data og informasjon at det er utfordrende å identifisere avvik, samt at det også utfordrer vår evne til å identifisere, sortere og dele informasjonen på tvers av sektorer.

Tverrsektoriell utveksling av informasjon og etterretning er en forutsetning for å skape en helhetlig maritim situasjonsforståelse. Totalforsvarskonseptet omfatter i dag gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn for å sikre best mulig utnyttelse av samfunnets begrensede ressurser når det gjelder forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret (FD/JD, 2015, s. 16). Dette organiseres prinsipielt ved bruk av krisehåndteringsprinsippene. *Ansvarsprinsippet* betyr at samme organisasjon har ansvar og myndighet for et fagområde i både normal- og krise-situasjoner. *Likhetsprinsippet* betyr at kriseorganisasjonen skal være så lik som mulig den daglige organisasjonen. *Nærhetsprinsippet* betyr at kriser skal organisatorisk håndteres på lavest mulige nivå, og *Samvirkeprinsippet* stiller krav til at alle virksomheter i forvaltningen har et selvstendig ansvar for å sikre godt samvirke andre relevante aktører i forebygging, beredskap og krisesituasjoner (FD/JD, 2015, s. 17). Samarbeid mellom relevante aktører ivaretas ved direkte samarbeid, og gjennom en rekke organer for samarbeid innenfor totalforsvaret (FD/JD, 2015, s. 18). På en annen side gir de irregulære kapabiliteter som Russland har i sin verktøykasse mulighet for både tvetydighet og mulighet for russiske myndigheter å fornekte kapabilitetens eksistens (Hicks, 2018, s. 7). Dette peker tilbake på Diesens poeng innledningsvis i kapittel 2 om at det kan bli utfordrende å fastslå om det pågår angrep eller ikke, samt at det vil være utfordrende å slå fast hvem som står bak, avhengig av om hendelsene er attribuerbare eller ikke-attribuerbare. Dette vil forsinke enhver beslutningsprosess. I tillegg vil juridiske bindinger internt mellom sektorer, for eksempel rundt skjermingsverdig informasjon, vilje til å dele, samt tverrsektoriell forståelse av hvordan «min lille del» av bildet kan ha en betydning i den store sammenhengen være utfordrende. Som rapporten «Contested Seas» tar opp er et viktig spørsmål om innsamlingskapasitetene og

sensorarkitekturen gir dekningen og evnen til å handle som nødvendig for å møte de truslene vi står overfor (Hicks, 2018, s. 2). Videre er det viktig å spørre seg om analysekapasiteten er i stand til å inkorporere de mange sensorene fra de mange aktørene for å skape tidsriktig og anvendbare analyser og brukbar etterretning. Til slutt må vi vurdere om den totale billedbyggingsprosessen for å skape maritim situasjonsbevissthet gir hensiktsmessige resultater og er rustet for både fredstid og krig, og om politisk, lovmessig og operasjonelt rammeverk er på plass for å kunne agere effektivt overfor en potensiell trussel (Hicks, 2018, s. 3).

## 4.5 Delkonklusjon

Norges maritime interesseområder består av store havområder, hvor det kan være utfordrende å skape en maritim situasjonsbevissthet for alle involverte. Dette kapittelet har først beskrevet hvordan maritim situasjonsbevisshet skapes i dag og drøftet noen av utfordringene knyttet til i hvilken grad vi er rustet til å kartlegge hybride trusler i det maritime domenet.

Først ble aktører og systemer i maritim forvaltning presentert sammen med de overordnede prosesser og hvilke resultater dette gir i form av maritim situasjonsbevissthet. Deretter ble utfordringer knyttet til vår langstrakte kyst diskutert i lys av russisk helhetlig tilnærming, for å danne et bilde av i hvilken grad vi i dag er i stand til å kartlegge hybride trusler. Dette er viktig for å vurdere hvordan bruk av stordata og SNA kan være en relevant metode for å øke maritim situasjonsbevissthet. Hovedutfordringen i dag er å gi tilstrekkelig fokus og prioritere begrensede ressurser mot de delene av det maritime domenet som trenger det til enhver tid. Med en russisk helhetlig tilnærming til konflikt kan det hevdes at dagens metode for å skape situasjonsforståelse kan hindre tidsriktig deling av informasjon internt i Forsvaret som organisasjon samt på tvers av sektorer. Samarbeidet mellom Forsvaret og andre sivile aktører og etater utvikles stadig, og systemer forbedres. En rekke aktører bidrar til å skape en best mulig felles forståelse, men det eksisterer fremdeles utfordringer med deling av relevant og tidsriktig informasjon i den hensikt å få oversikt i det komplekse maritime domenet.

I lys av russisk helhetlig tilnærming vil bruk av irregulære virkemidler gjøre det utfordrende å detektere avvik fra normalsituasjonen. Det vil da kunne oppstå utfordringer med å skille uskyldige hendelser fra hendelser med hybrid karakter, og med bruk av fordekte sivile aktører i et komplekst operasjonsområde kunne utfordre vår maritime situasjonsforståelse.

# 5 Hva kan AIS-data gi oss?

Denne delen av studien bidrar til grunnleggende informasjon om AIS som system, og hvilke egenskaper ved dette systemet som gjør det relevant som analyseobjekt i SNA. Den første delen av dette kapittelet vil omhandle AIS generelt, mens den siste delen tar for seg tidligere studier og påviste feilkilder med bruk av AIS som datagrunnlag.

Automatic Identification System (AIS) ble innført av IMO i 2004 som et antikollisjonssystem for å øke sikkerheten til sjøs, og inngår i Forsvarets generelle overvåkning av våre interesseområder. AIS mottakere langs kysten registrerer fartøy innenfor 40-60 nautiske mil, og med satellittbaserte systemer er en i stand til å følge trafikk over alle hav.

Systemet foretar en forhåndsprogrammert utsending av to ulike former for data: statiske, og dynamiske (øvrig informasjon knyttet til sjøreisen). *Statiske* AIS-data består av Maritime Mobile Service Identity nummer (MMSI), kallesignal og navn, IMO-nummer, lengde og bredde, type fartøy, og lokalisasjon av posisjonsantenne (IMO, 2015, s. 5). Statiske data blir sendt ut automatisk med en datafrekvens på 6. minutt eller på forespørsel (IMO, 2015, s. 7). *Dynamiske* data består av fartøyets posisjonsdata, fartøyets kurs «over grunnen» (COG), heading, navigasjonsmessig status (for eksempel «til ankers» eller «underveis ved bruk av motorkraft»), og «rate of turn» (antall grader kursendring per minutt). Datafrekvensen for utsendelse av dynamiske data blir avgjort av fart og kursendringer. Et fartøy til ankers vil sende informasjon hvert 3. minutt, mens et fartøy underveis vil sende ut informasjon hvert 2. til 10. sekund avhengig av hvilken kurs eller fart det aktuelle fartøyet har (IMO, 2015, s. 7). AIS er av kommunal og moderniseringsdepartementet definert til å være en viktig stordatakilde for etatene i maritim forvaltning (Vivento, 2015, s. 33).

Kystverket drifter i dag et satelittsystem som siden 2010 har monitorert sivil skipstrafikk med spesielt fokus på de deler av norske interesseområder som ikke er dekket av landbaserte AIS-stasjoner. Systemet består i dag av 4 satellitter. Disse er et samarbeidsprosjekt mellom FFI, Kongsberg, Kystverket og Norsk Romsenter (Kystverket, 2017a).

IMO refererer til SOLAS-konvensjonen av 1974 når de understreker regelverkets påbud om at alle fartøy fra 300 bruttotonn og oppover i internasjonal fart, handelsfartøyer på 500 bruttotonn og oppover uavhengig av internasjonal fart samt alle passasjerfartøy uavhengig av størrelse er pliktig å ha installert AIS om bord (IMO, 2015, s. 1). I analysedelen i kapittel åtte fokuseres det på fartøysnavn, MMSI-nummer, IMO-nummer, fartøystype, posisjonsangivelse, fart (SOG), samt tidsangivelse (UTC). Disse data vil kunne gi relevant informasjon som kan knytte fartøyene sammen i nettverk og gi opplysninger om eierstruktur.

# 5.1 AIS-informasjon

Ved å analysere AIS-utsendelser i hele det norske interesseområdet for både 2014 og 2017 var det mulig å skape en nær komplett logg over maritim trafikk med eksakt dato, tid og lokasjon. AIS-informasjonen gav unik identifikasjonsinformasjon for hvert skip av interesse.

## MMSI-nummer

Et fartøy identifiseres med navn og kallesignal. Et fartøys MMSI-nummer er en unik kode bestående av ni siffer som er internasjonalt entydig identifikasjonsnummer for hvert enkelt fartøy. Ut i fra MMSI-nummeret er det mulig å avdekke fartøyets eier, og MMSI-nummeret kan endre seg ved eierskifte på et fartøy.

MMSI-formatet er slik: MID 259041000, hvor MID (Maritime Identification Digit) definerer skipets identitet (I dette eksempelet den norske fregatten KNM Fridtjof Nansen). MID tildeles i Norge av Telenor Maritim Radio, og internasjonalt av ITU (International Telecommunication Union). Norge har som en stor sjøfartsnasjon fått tildelt MID 257, 258 og 259. Russland har MID 273. Det første sifferet angir verdensdel, de to neste landet (FalckNutec, 2014, s. 10).

## IMO-nummer

Et fartøys IMO-nummer er en unik kode bestående av syv siffer. I motsetning til MMSI-nummeret blir IMO-nummeret permanent tildelt fartøy uavhengig av eier. Regelverket omfatter alle fartøy fra 100 bruttotonn eller mer, samt fiskefartøy, passasjerfartøy (ned til 12 meters lengde) og borerigger i internasjonal seilas. SOLAS-reguleringen fritar enkelte fartøy fra kravet. Dette gjelder fartøy som ikke har maskinell fremdrift, lystbåter, spesielle fartøy (eksempelvis SAR-fartøy), mudringslektere, flytedokker, krigsskip, og fartøy med konstruksjon av tre og som samtidig ikke er fiskefartøyer (IMO, 2017, s. 3). IMO-nummeret følger fartøyet gjennom dets levetid, og skal bestå uavhengig om enheten skifter eier.

## Speed over ground (SOG)

Speed Over Ground, er fart «over grunnen» og gjengir den farten et fartøy beveger seg relativt i forhold til jorden. Farten beregnes ut ifra relative krefter som ytre påvirkning fra vind eller strøm. Hvis et fartøy har 13 knop gjennom vannet og motstrømmen er 3 knop vil fartøyet ha en fart på 10 knop over grunnen (SOG).

### Course over ground (COG)

Course over ground, er kurs «over grunnen» og gjengir den kursen fartøyet beveger seg relativ i forhold til jorden. Kursen beregnes ut i fra relative krefter som ytre påvirkning fra vind eller strøm, uavhengig av hvilken faktisk retning (true heading) baugen på fartøyet måtte ha.

### UTC

Tidsangivelse ved bruk av UTC beskriver tid med år, måned, dag, time, minutt og sekund.

## 5.2 Tidligere forskning

Studien av «The Odessa Network: Mapping Facilitators of Russian and Ukrainian Arms Transfers» ble gjennomført av tenketanken C4ADS, hvor Tom Wallace og Farley Mesko kartla kommersielle maritime nettverk med bindinger til den russiske stat og deres involvering i våpentransport. Nettverket i Odessa-rapporten fraktet sensitiv last i form av våpen ut fra Ukraina i regi av russiske myndigheter. Wallace og Mesko avdekket i forbindelse med studien utfordringer med å benytte AIS som datagrunnlag. Fartøy kan slå av utsendelse, kringkaste feil informasjon eller «spoofe» signaler slik at det fremstår som om de er et helt annet sted enn hvor de egentlig befinner seg. Konkrete eksempler på dette er iranske fartøy. Disse identifiseres i Odessa-studien som regelmessige lovbrytere ved å spoofe signaler. Det russiske fartøyet «*Professor Katsman*» forsøkte å skjule sin delaktighet i russisk våpentransport til Syria ved å slå av AIS (Wallace & Mesko, 2013, s. 67-68). Det finnes feilkilder i AIS systemet. Når et fartøy er langt til havs kan det være utfordringer med å gjennomføre mottak av AIS signalene. Det samme gjelder havner i underutviklede områder. Odessastudien viser, at til tross for at dekningsgraden ikke var feilfri i 2013, var antallet steder der man ikke hadde dekning relativt få (Wallace & Mesko, 2013, s. 68).

Forsvarets Forskningsinstitutt (FFI) driver også omfattende forskning på AIS og feilkilder knyttet til systemet. Rapportene fra FFI er graderte på en slik måte at det ikke vil være mulig å gjengi dem i denne studien. En studie gjennomført av det israelske selskapet Windward, som samler inn og distribuerer AIS-informasjon til kunder i hele verden som har interesser i skipstrafikken, har laget en oversikt over avvik i AIS-informasjonen (Windward, 2014).

## 5.3 Avvik i AIS informasjon

I Windwards rapport som er inkludert i forskning på FFI er de mest sentrale funn på avvik i AIS-informasjon som følger.

## Falsk identitet

Identiteten til et fartøy angis med informasjonen (MMSI, IMO nummer) som er beskrevet tidligere i dette kapittelet. Rapporten fra Windward peker på at bruken av falsk eller stjålet identitet er et økende problem, og at 1% av fartøyene på verdensbasis er berørt. Dette sammenlignes med at 1000 mennesker passerer gjennom John F. Kennedy Intl. Airport med falsk identitet hver dag (Windward, 2014, s. 4).

## Skjuler destinasjon

Rapporten hevder at fartøyer bare i 41% av tiden rapporterer endelig destinasjon. Denne informasjonen skal være inkludert i data som AIS-transponderen sender ut. Dette kan føre til misledende informasjon (Windward, 2014, s. 4).

## Slår av AIS – «going dark»

Rapportens funn viser at mer enn 25% av fartøyene skrur av AIS i minst 10% av tiden. Dette er mer vanlig blant fartøy på over 250 meter. Windward peker på at dette indikerer at fartøyene som bærer den største lasten har større insentiver til å skjule sine aktiviteter på enkelte tidspunkt (Windward, 2014, s. 4). Dette korrelerer med funnene i Odessa studien.

## Manipulering av GPS data

AIS-senderen foretar ingen validering av GPS-data. Derfor er det slik at et hvilken som helst posisjonsinput som blir gitt inn i AIS-senderen vil bli sendt ut som skipets posisjon, uavhengig av skipets reelle posisjon. Rapporten viser til at i perioden 2013-2014 har det blitt registrert en økning på 59% i manipulering av AIS-data. Denne type manipulering kan få det til å se ut som et fartøy er på helt andre steder enn der det virkelig befinner seg (Windward, 2014, s. 5).

## Juksing med AIS («spoofing»)

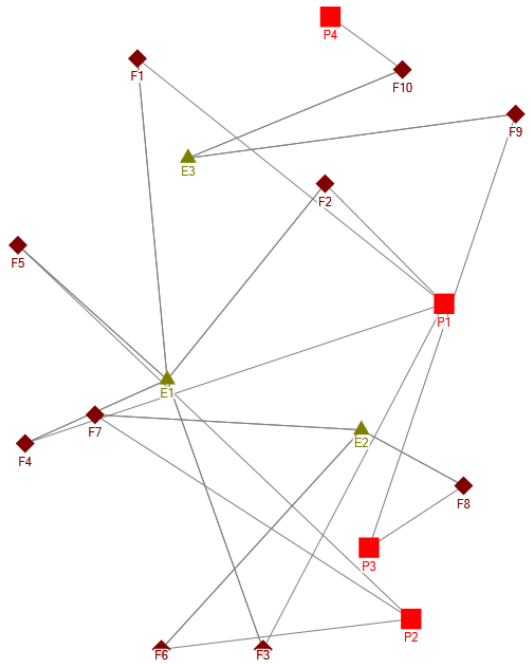
I følge rapporten har det blitt påvist at en kan hacke datastrømmen i fra AIS ved at det for eksempelvis genereres «spøkelsesskip» – fartøy som i virkeligheten ikke eksisterer. Videre kan man ved å «spoofe» signaler generere falsk støy i AIS-bildet som negativt kan påvirke den maritime situasjonsforståelsen (Windward, 2014, s. 5). Denne type aktivitet ble oppdaget i Odessa-rapporten ved gjennomføring av russiske og iranske våpentransporter. Det tidligere nevnte fartøyet *«Professor Katsman»* var et av fartøyene som, etter å ha forlatt Oktyarbrsk (Ukraina), entret Middelhavet og forsvant fra AIS-bildet i ukesvis (Wallace & Mesko, 2013, s. 68). Både eksisterende systemer i dag, samt analyseverktøyet brukt i denne oppgaven vil ha filter som fanger opp unormal «adferd» generert av spoofing.

## 5.4 Delkonklusjon

Påbudet om å installere og bruke AIS er nedfelt i SOLAS kapittel V. AIS kan gi oss verdifull informasjon i analyse av problemstillinger tilknyttet det maritime domenet. Funnene fra både Odessa studien og Windward rapporten viser imidlertid at det allikevel finnes en del feilkilder i systemet, som i tillegg til tekniske feil ofte kan tilskrives bevisste eller ubevisste menneskelige feil. Feilkildene vil kunne påvirke datasettet som er omhandlet i denne studien, og at tilliten til AIS-systemet som sådan forringes. Dette er viktig å ta med seg inn i en analyse av denne type data.

# 6 Sosial nettverksanalyse (SNA)

Begrepet *nettverk* har de siste tiårene vært et av de mest utbredte begrepene i sosialvitenskapen (Raab & Milward, 2003, s. 417). Dette kapittelet tar for seg grunnleggende og sentrale begreper innen nettverksteori som er relevante for denne oppgaven. Et sosialt nettverk er satt sammen av aktører og de ulike båndene som knytter dem sammen. Aktørene blir ofte kalt noder og kan bestå av personer, organisasjoner eller konsepter (Borgatti & Foster, 2003, s. 992). Nodene eller medlemmene i nettverket er knyttet sammen med relasjoner eller bånd (Golbeck, 2013, s. 2). Nettverksanalyser gir slik en mulighet til å gjøre en abstraksjon, ved å analysere strukturen i et nettverk, og ikke innholdet. Den enkleste formen for struktur som kan utgjøre et nettverk er en dyade, som er et par (bestående av to noder) og båndet som eksisterer mellom dem. Båndene varierer med både type, retning og styrke. Ved analyse av nettverk må analytikeren bestemme hva som skal til for at to enheter har en relasjon enten det er snakk om følelsesmessige (som vennskap) til rollebaserte (slektsforhold), ressursbaserte (finansiell strøm) samt grad av tilhørighet (medlem av samme menighet, klubb eller terroristgruppe) (Cunningham et al., 2016, s. 10). Definisjonen av en relasjon vil ha stor betydning for hvordan en visuell fremstilling av et nettverk, et sosiogram, vil være. Hvordan er dette overførbart til kartlegging av mørke eller grå maritime nettverk?




Figur 6.1 Fiktivt maritimt nettverk. F=Fartøy (1-10), E=Eier (1-3), P=Posisjon(1-4)

## 6.1 SNA – konsept og terminologi

I faglitteraturen blir ofte Georg Simmel trukket frem som konseptets grunnlegger. Han studerte hemmelige samfunn og bidro til ny innsikt i hemmelige samfunns organisering (Everton, 2012, s. 3; Simmel, 1906). Metoden har utviklet seg videre der blant annet den moderne sosiologien med sosiologen Harrison White i spissen har hatt en sentral rolle. Han utviklet på 1960- og 70-tallet teknikker for å forstå sosiale relasjoner og hvilke mønster som utvikler seg i et sosialt nettverk (Cunningham et al., 2016, s. 3). I studien «Dark Networks as problems» beskriver Raab og Milward nettverksanalyse som en av de viktigste nyskapningene innen sosialvitenskapen de siste tretti årene. Samme studie viser hvordan bruksområdet for metoden har vokst for eksempel ved analyse narkotikanettverk, terrornettverk som Al-Qaida, og nettverk som driver våpensmugling i Vest-Afrika (Raab & Milward, 2003, s. 420).

I dag er SNA en samling av teorier som danner et metodisk grunnlag for empiriske studier av hvordan og hvorfor nettverk av relasjoner dannes og for beskrivelser av disse strukturene (Everton, 2012, s. 5). Fordi nettverkskonseptet baserer seg på relasjonen mellom aktører istedenfor egenskaper som alder og kjønn, blir det mulig for forskere å analysere sosiale relasjoner og sammenhenger (Raab & Milward, 2003, s. 417). SNA fokuserer på studien av relasjonelle strukturer, og èn måte å forstå dette på er at sosiale nettverk er bygget opp av *aktører* og *båndene* mellom dem (Cunningham et al., 2016, s. 10). Slik tilfører disse teoriene og teknikkene empirisk innhold til sosial kontekst (Everton, 2012, s. 7). Et system med entiteter og relasjoner mellom disse kan representeres matematisk og visuelt ved en *graf*. Informasjonen sammenfattes systematisk for å kunne fremstille resultater, og funn kan gjøres eksempelvis i matriser, grafer eller sosiogrammer. Dette kan gi informasjon om mønstre av relasjoner i et nettverk. Interessen har i de senere år økt kraftig i ulike vitenskapelige miljøer, og vært brukt innen en rekke områder for kartlegging av slike nettverk innen en rekke disipliner (Everton, 2012, s. 4-5).

Det er også behov for å presisere hva begrepet ikke er. Andre analytiske metoder som for eksempel link analyse fokuserer på relasjoner mellom ulike objekter. Der SNA gir en analytisk mulighet til å kvantifisere og måle relasjoner mellom like aktører (epler mot epler), tilbyr link analyse kun mulighet til å sammenligne bånd mellom objekter av ulik karakter (epler mot appelsiner). Ved å rendyrke entiteter gir det oss mulighet til å kvantifisere ulike relasjoner mellom dem (Cunningham et al., 2016, s. 7). SNA kan også lett bli mistolket til å dreie seg om sosiale medier og analyse av disse. Dette er ikke det samme, selv om SNA også kan brukes til å kartlegge sosiale medier (Cunningham et al., 2016, s. 6). Strukturen består i antallet noder,

antallet bånd mellom dem og avstanden mellom de ulike nodene. Innholdet beskriver således betydningen av relasjonen mellom nodene, samt andre karakteristika som flyten og distribusjonen av informasjon, ressurser og grad av påvirkning (Balkundi & Harrison, 2006, s. 4; Cunningham et al., 2016, s. 13).

## Grafteori

En graf er i denne sammenheng en visuell modell av et sosialt nettverk bestående av noder med forbindelser mellom enheter (Cunningham et al., 2016, s. 10; Everton, 2012, s. 400). En direktiv/retningsbestemt forbindelse (ofte kalt *pil*) vil si at den har en startnode og en ende-node og peker fra en node til en annen (Everton, 2012, s. 399). Dersom en linje mellom to noder er ikke-direktiv/ikke-retningsbestemt kalles dette en *kant*. Mørke nettverk vil av natur forsøke å operere fordekt eller skjult. Relasjoner i slike nettverk vil derfor ofte være utfordrende å kartlegge, og dermed ofte bli behandlet som *ikke-retningsbestemte* (Cunningham et al., 2016, s. 10). Man vil på grunn av dette ikke få en «ekte» representasjon av det virkelige nettverket, bare en analytikers fremstilling av det. I konteksten til oppgaven og analyse av AIS-data vil fokuset være på å finne forbindelser mellom fartøy, selskaper og interessante geografiske områder, for å bli i stand til å se hvordan nettverket utvikler seg over tid.

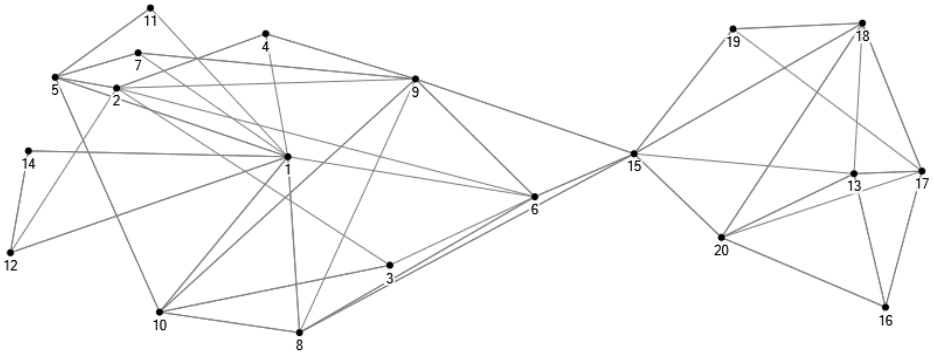
Figur 6.2 Ikke-direktiv kant mellom to noder

Figur 6.3 Direktiv kant mellom to noder

## Betydningen av bånd

Sterke bånd er ifølge Everton en repetitiv og relativ intens interaksjon mellom to noder, mens svake bånd knytter noder som har mindre hyppig eller sjeldnere kontakt. I sin studie av 11. september nettverket kom Valdis Krebs frem til at nodene utviklet ulik grad av bånd basert på tid tilbrakt sammen (bodde sammen, reiste sammen, eller hadde kortere møter) (Krebs, 2002, s. 47). I slike nettverk vil nodene sjelden være tilfeldig plassert. Som Everton beskriver det, vil nodene samle seg i såkalte *«cluster» eller klynger*, og danne relativt distinkte sub-grupper eller undergrupper (Everton, 2012, s. 10). Når disse er så tett sammenvevde at alle nodene er i kontakt med alle kalles de *klikker*. Kjennetegnet ved disse er at man ikke kan tilføre eller ta bort noen av nodene i klikken uten å endre særegenhetene ved denne (Cunningham et al., 2016, s. 116). Mellom disse klikkene kan man finne forbindelser med relativt lav kontaktflate og som tetter gap

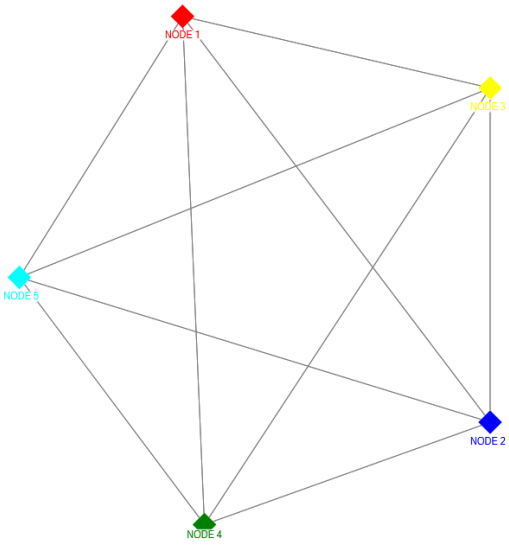
i et sosialt nettverk (Cunningham et al., 2016, s. 11). *Broer* er kanter/noder som forbinder to deler av et nettverk som for øvrig ikke er forbundet til hverandre, mens «brokers», eller *nettverksmeglere* er nodene på hver side av en slik bro. Både broer og «brokers» er i posisjon til å kontrollere flyt av ressurser gjennom nettverket (Everton, 2012, s. 13). I figur 6.4 er kantene mellom node 15, 6, 8 og 9 broer, mens selve nodene kalles «brokers».



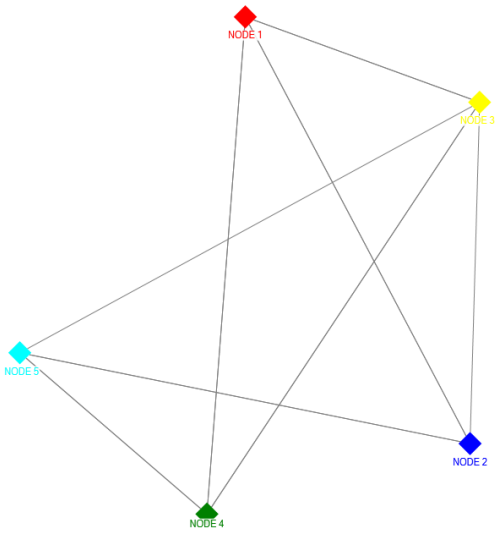

Figur 6.4 Hypotetisk sosialt nettverk

## Tetthet i nettverk

Kanter representerer som vi har sett tidligere en relasjon. Tetthet er summen av alle *kanter* delt på antall mulige kanter i et nettverk, og gir oss innsikt i hvor tett forbundet nettverket er (Everton, 2012, s. 11; Kadushin, 2012, s. 29).




Figur 6.5 Hypotetisk nettverk. Tetthet = 1




Figur 6.6 Hypotetisk nettverk. Tetthet = 0,8

I et nettverk kan altså samtlige noder være forbundet til alle andre aktører (Cunningham et al., 2016, s. 98). Dette er et viktig måling fordi det kan brukes til å si noe om tilliten som eksisterer i nettverket samt hvor synlig nodene i det respektive nettverket er (Kadushin, 2012, s. 29).

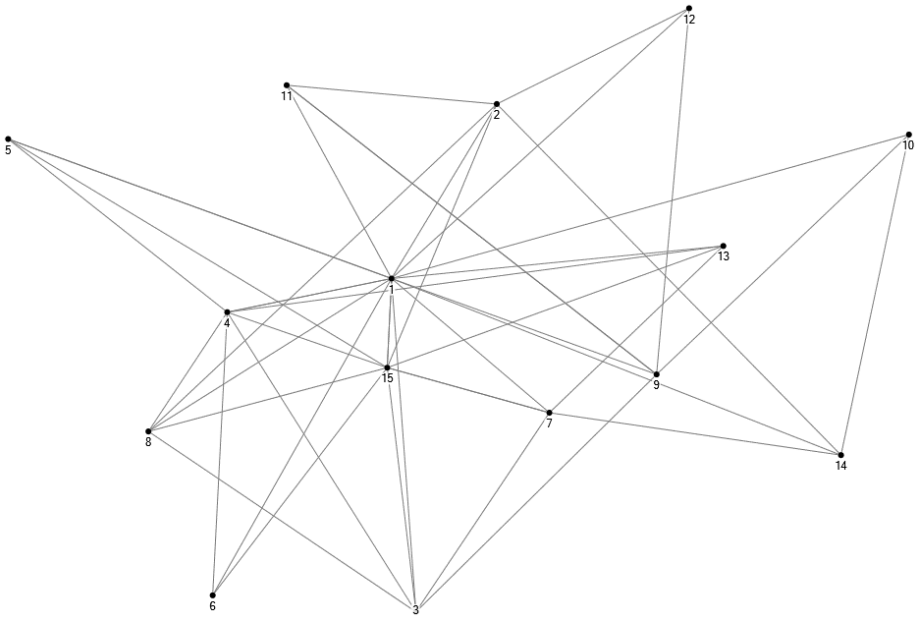
Dersom ingen i nettverket er knyttet sammen er tettheten 0. Dersom alle i nettverket er knyttet sammen gjennom alle mulige bånd, er den 1 (Everton, 2012, s. 146).

## Strukturelle hull

Tetthet er et uttrykk for hvor godt sammenknyttet nettverket er. Men, som Kadushin viser til i sin referanse til forskningen gjort av Ronald S. Burt (1992), kan man snu konseptet på hodet og studere mangelen på sammenknytning i nettverk (Kadushin, 2012, s. 29). Argumentet er at sterke bånd med andre noder resulterer i mindre nytteverdi fordi sterke bånd eksponerer en for den samme informasjonen igjen og igjen (De Nooy, Mrvar & Batagelj, 2018, s. 138). Cunningham refererer til Ronald Burts forskning for å forklare begrepet strukturelt hull. Han forklarte dette som et gap i en nettverksstruktur som er tettet av en såkalt bro. Ego-noder (noden, nærliggende noder og båndene i mellom dem) som bare har et eneste bånd til en annen node indikerer tilstedeværelse av et strukturelt hull.

## Stier (path) og avstand (path distance)

En *sti* er en sekvens av noder og forbindelser man kan krysse og måle ved å følge *kantene* mellom to sammenknyttede noder i et nettverk (Cunningham et al., 2016, s. 403). Man er som regel interessert i den korteste *stien* mellom to noder, og følger derfor stien som en node har måttet gå for å kontakte en annen node i nettverket. Avstanden mellom et par enheter i nettverket kalles avstand, og består av antall kanter mellom nodene (Cunningham et al., 2016, s. 402; Golbeck, 2013, s. 20). I figur 6.7 kan man følge stien mellom node 10 til node 7 og fra node 11 til node 15. I begge tilfeller er avstanden 2. Den korteste stien i et nettverk kalles geodetisk avstand (Kadushin, 2012, s. 33).




Figur 6.7 Illustrasjon av sosialt nettverk. Nettverket består av 15 ulike noder og relasjonene mellom dem.

## Sentralitetsbegrepet

I kartlegging av dark networks kan det være ønskelig å kartlegge hvilke node eller aktører som innehar posisjonen som den «viktigste» i nettverket (Kadushin, 2012, s. 31). Sentrale noder i for eksempel terrornettverk har som regel tilgang til både informasjon og ressurser på et høyt nivå i nettverket (Perliger & Pedahzur, 2011, s. 48). Sentralitet, eller «popularitet», er en måling av hvilke noder som har flest forbindelser til andre noder og dermed blir det teorien kaller *sentral* i nettverket. I figur 6.7 ser vi at node 1 og 15 har flest forbindelser og dermed regnes som nodene med høyest sentralitet. Oppgaven tar utgangspunkt i Freemans forståelse av sentralitetsbegrepet. Han skiller mellom gradssentralitet, mellomleddsentralitet og nærhetssentralitet (Freeman, 1979, s. 237). Som Everton legger frem har en sentral node i et maritimt nettverk på grunn av sin posisjon lettere tilgang til ressurser samt at de er effektive i å spre informasjon til andre noder (Everton, 2012, s. 12).

**Gradssentralitet (Degree Centrality),** er et mål på hvor mange forbindelser en spesifikk node har. Node nummer 1 har i figur 6.7 en gradssentralitet på 14. Utregning av gradssentralitet vil kunne gi indikasjoner på nodens aktivitet i nettverket, samt den direkte innflytelsen eller makten den aktuelle aktøren er i stand til å utøve i nettverket. (Cunningham et al., 2016, s. 144)

**Mellomleddsentralitet (Betweeness),** er relatert til i hvilken grad en node i et nettverk ligger langs den korteste «stien» som forbinder alle andre par med noder i nettverket (Everton, 2012, s. 397). Man kan nå andre noder i nettverket via disse. I denne studien vil dette være interessant å finne ut om enten fartøy eller selskaper i eierstruktur har høy grad av mellomleddsentralitet, da

dette kan si noe om hvilke noder som er sentrale for å komme i kontakt med andre deler av nettverket (Kadushin, 2012, s. 32).

**Nærhetssentralitet,** måler gjennomsnittlig avstand fra en spesifikk node til andre noder i nettverket (Cunningham et al., 2016, s. 150). Nærhet kan forstås som et mål på tiden det tar før noden man fokuserer på når ut til de andre nodene i nettverket den er i forbindelse med. I en studie av maritime nettverk som dette vil dette kunne måle den kapasiteten en spesifikk node har til å påvirke resten av nettverket (Everton, 2012, s. 209).

### Grad av kohesjon

Sosiale nettverk inneholder ofte klynger med noder som «holder sammen» i «clusters». Sosiale nettverksanalytikere refererer gjerne til klynger med stor tetthet hvor det er sterke, positive, direkte og intense bånd som kohesive subgrupper eller subnettverk. Sosial interaksjon danner så grunnlaget for solidaritet, normer og identitet (Everton, 2012, s. 12). På denne måten vil aktører som har intensiv interaksjon kalle seg selv en *sosial gruppe* (De Nooy et al., 2018, s. 61). I denne studien vil klynger kunne oppstå når man analyserer fartøy som oppholder seg i samme interesseområde, eller helt enkelt fartøyer som ligger til kai i nærheten av hverandre i samme havn.

### Roller og posisjoner

Rollebegrepet brukes i denne sammenheng om relasjoner mellom noder i hele nettverk (Kadushin, 2012, s. 38). SNA fokuserer på både de direkte og indirekte båndene mellom aktører og forklarer adferden og de sosiale prosessene mellom nodene i lys av dette (Everton, 2012, s. 13). I maritime nettverk har man også avdekket sosiale strukturer som for eksempel er knyttet til håndtering av sensitiv last der selskaper med spesielle roller innen våpentransport viser seg å ha svært mange innbyrdes forbindelser ved at personell i nettverket er i familie, er tidligere klassekamerater, nære venner og så videre (Wallace & Mesko, 2013, s. 4). På den andre siden skiller begrepet posisjon seg ut på den måten at i stedet for å fokusere på bånd mellom aktører, ønsker man å identifisere noder i nettverket som er strukturelt likeverdige. For eksempel eiere i eierstrukturer i maritime nettverk som er strukturelt likeverdige, vil opptre i samsvar med hverandre uavhengig om det eksisterer et bånd mellom dem eller ikke (Everton, 2012, s. 12).

## 6.2 SNA – utvalgte caser

Har metoden og måleparameterne i sosial nettverksanalyse som denne delen av oppgaven hittil har tatt for seg overføringsverdi til kartlegging av mørke og grå maritime nettverk i norske interesseområder? La oss først se på et utvalg av historiske eksempler, der SNA har vært brukt i

forskning som kan ha overføringsverdi til maritim situasjonsbevissthet og kartlegging av maritime hybride nettverk.

Kartlegging av «mørke nettverk» har blitt gjennomført i flere tilfeller som har overføringsverdi til denne studien. Terrorangrepene 11. september 2001 gjorde at et større publikum fikk oppmerksomheten opp for det ødeleggende potensiale i organisasjonsformen til slike nettverk. Studien til Valdis E. Krebs var en viktig faktor i å anvende SNA for kartlegging av «mørke nettverk». Krebs gjennomførte i etterkant av angrepene en SNA av kaprernettverket. De 19 kaprerne og deres relasjoner seg imellom ble kartlagt. Mohammed Atta har gjennom den offisielle etterforskningen blitt utpekt som hovedmann bak angrepet. Gjennom analysen ble han identifisert som nettverkets node med høyest grads- nærhet- og mellomsentralitet, noe som bekrefter hans status. Til tross for dette utelukker ikke Krebs at nettverkets struktur med målt sentralitet vil endre seg drastisk dersom man oppdager nye forbindelser i nettverket i fremtidig etterforskning. Denne studien ble for øvrig gjennomført ved innsamling av data fra åpne kilder (Krebs, 2002, s. 47).

I den tidligere nevnte studien «The Odessa Network» stilte Wallace og Mesko spørsmålstegn til hvordan russiske- og ukrainske våpenlaster kommer seg fra A til B. Denne studien, som utelukkende var basert på åpne kilder, samlet store mengder data om det maritime nettverket som sto bak transporten. Ved bruk av SNA kartla og dokumenterte studien over førti tilfeller av selskaper med ulik tilknytning til statlige aktører i Russland eller Ukraina. En relativt liten gruppe selskaper og individer både fra Ukraina og EU med tette bånd og høy grad av tillit til både hverandre og høytstående embedsmenn i både russiske myndigheter og i regional militærindustri sto bak (Wallace & Mesko, 2013, s. 74). En rekke avvik ble avdekket i studien, der et av de mest interessante funnene er hvordan disse nettverkene angivelig ønsker å holde seg i det skjulte (derav dark maritime networks) ved å slå av AIS under transit mot destinasjoner som for eksempel Syria (Wallace & Mesko, 2013, s. 68). En uidentifisert norsk havn ble avdekket og skal ha blitt brukt av nettverket (Wallace & Mesko, 2013, s. 21).

Naval Postgraduate School (NPS) er et universitet i US Navy som utdanner militært personell på mastergrads- og doktorgradsnivå. Her drives forskning som har til hensikt å øke effektiviteten til det amerikanske forsvaret. Universitetet har benyttet SNA for å kartlegge og forstyrre terrornettverk, IED (Improvised explosive device) nettverk, cyber nettverk samt kriminelle nettverk. NPS kunngjorde som tidligere nevnt studien «Mapping Dark Maritime Networks» i april 2018. Studien identifiserte 314 kinesiske fartøyer som deltok i mudring, og oppbygging av kunstige øyer i Sør-Kina-havet. Studien ble ledet av Dr. Wayne Porter ved

Littoral Operations Center støttet av analytikere ved CORE Lab (analyseavdeling ved NPS). Hensikten var å øke US Navy sin operasjonelle kapasitet til å overvåke den kinesiske aktiviteten (Porter et al., 2018, s. 2). Studien er således det første kjente forskningsprosjektet der AIS data dannet grunnlag for sosiale nettverksmatriser brukt til maritim nettverksanalyse bestående av fartøy, operatører, eiere, havner og kunstige øyer. Studien tok for seg 18 måneder med data som strakte seg fra november 2014 til mars 2016. I perioden ble nettverksstrukturer for fartøyer involvert i kinesiske «grå nettverk» etablert med utgangspunkt i deres samlokalisering over de geografiske områdene hvor Kina i dag etablerer kunstige øyer (Porter et al., 2018).

## 6.3 Delkonklusjon

Dette kapittelet har gitt en oversikt over sentrale elementer innen SNA i den hensikt å skape forståelse for hvordan metoden benyttes som fundament i oppgavens analysedel. Maritime aktivitet i våre interesseområder består ulike former for nettverksstrukturer. Ved å kartlegge nettverkets struktur kan man identifisere sentrale noder. Kartlegging av noder, deres relasjoner og sentrale aktører i nettverk kan slik bidra til dypere forståelse av dynamikken i komplekse strukturer. Denne litteraturgjennomgangen viser at bruk av SNA kan bidra til å kartlegge maritime nettverk og forstå hvordan man best kan tilnærme seg disse for å unngå at de utnytter sine kapasiteter.

# 7 Stordata- og nettverksmetodikk

I dette kapittelet vil metodikk, programmering og design for bruk av stordata og konstruksjon av nettverksstrukturer bli presentert. Først vil det bli redegjort for analysens verktøy, programmeringsspråket R, samt de viktigste algoritmene (pakkene) som benyttes i studien. Deretter vil kriteriene som er lagt til grunn for modellering av maritime nettverk i oppgaven bli redegjort for, før logikken bak nettverkspresentasjonen blir beskrevet til slutt.

## 7.1 Utvikling av analyseverktøy - «R» og «Rstudio»

R, er et objektorientert programmeringsspråk som ble utviklet i 1996 av Ross Ihaka og Robert Gentleman (Linnarsson, 2015, s. 4). Utvikling og koding i R for å muliggjøre analysen ble gjennomført i samarbeid med teamet ved CORE[8] lab (NPS) og FFI. Systemet er fleksibelt og har blant annet programmeringsfunksjoner som muliggjør statistisk beregning, datamanipulasjon, kalkuleringer og grafisk visualisering av resultater i eksempelvis grafer og diagram (R-Project, 2018). Det er Rstudio som er blitt benyttet for kjøring av R i forbindelse med denne oppgaven. Rstudio er et integrert utviklingsmiljø for statistisk databehandling og grafikk. Videre har R har et eget bibliotek koblet til seg. Biblioteket heter CRAN (Comprehensive R Archive Network), og her kan man laste inn en rekke ulike pakker som er designet for bruk i R. Tilgang til CRAN gjøres direkte i R-applikasjonen (Linnarsson, 2015, s. 4).

### Leaflet

Leaflet er en av de mest benyttede JavaScript biblioteker for interaktive kart. Applikasjonen gjør det enkelt å integrere og kontrollere kart i R, og muliggjør generering av kart i Rstudio (Rstudio, 2018). Kartutsnittene i oppgaven er generert ved bruk av denne applikasjonen.

### T-Locoh

T-Locoh (Time Local Convex Hull) er en algoritme som implementert i R brukes til analyse av bevegelsesdata, og følging av for eksempel enheter som jevnlig sender ut sin GPS posisjon. R og T-Locoh har tidligere vært brukt til blant annet innen forskning på dyrs bevegelsesmønster (Eric, Colin, Jason & Wayne, 2017, s. 1). Bruk av denne algoritmen dannet gunnlaget for å visualisere polygon for alle fartøyer som manøvrerte saktere enn 1,5 knop.

[8] Common Operational Research Environment Lab. Etablert ved NPS i 2007. (https://my.nps.edu/web/core)

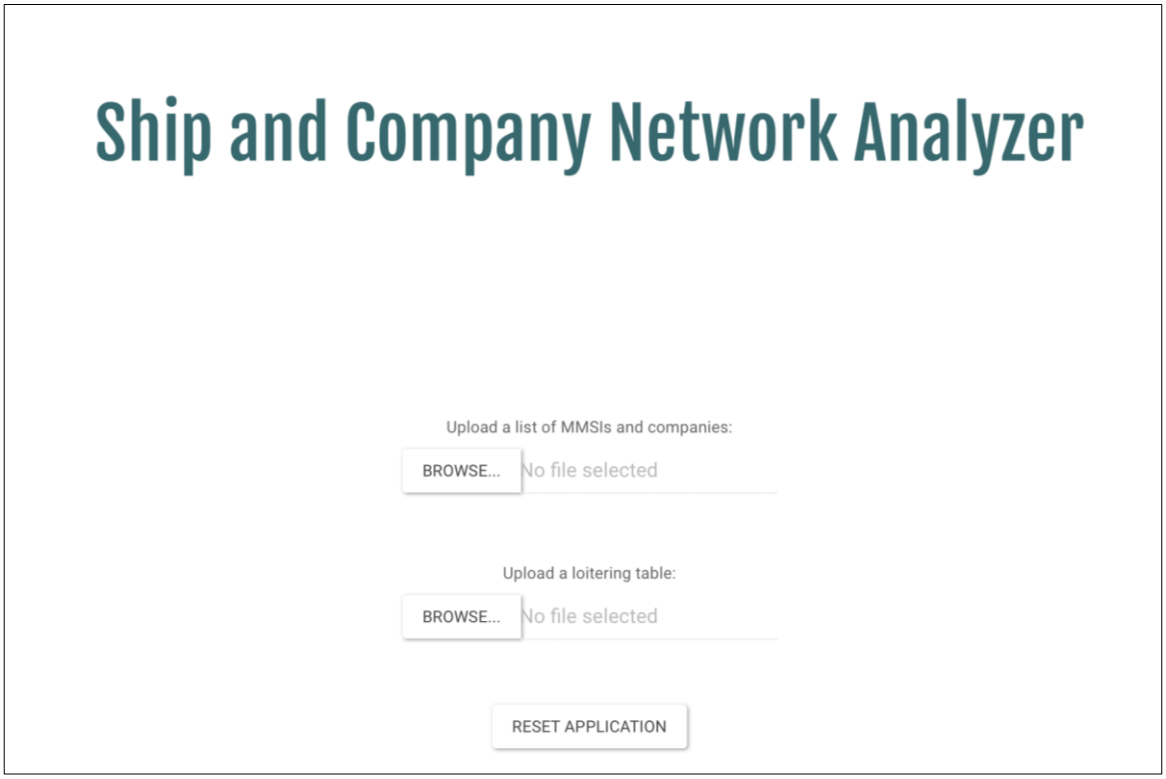
Figur 7.1 «T-Locoh» algoritmen gir visualisering av geospatielle data. Eksempelet er fra Andøya og viser blant annet geolokalisering av fiskeriaktivitet på Vesterålsbankene i mars 2017. Kartgrunnlaget er laget ved bruk av Leaflet for R (Rstudio, 2018).

Fartøy som ble registrert med stopp ble dersom de ble registrert i samme område knyttet til hverandre i et ikke-retningsbestemt nettverk. Prosedyren ble gjennomført for hver måned i henholdsvis 2014 og 2017.

## R-shiny

Shiny er en algoritme eller pakke til R som gir mulighet for visualisering av koding og analyseresultater i R. Basert på denne oppgavens fokusområde og problemstilling, videreutviklet teamet ved CORE lab NPS, med Rob Schroeder og Christopher Callaghan i spissen, den samme Rshiny applikasjonen som ble benyttet for NPS studien i Sør-Kina-havet. Applikasjonen leser input i form av *.xlsx (open XML spreadsheet file format used by Microsoft Excel) og *.csv (comma-separated value) filer:

1. Samtlige registreringer for fartøyers stoppunkter. Her linkes fartøyers MMSI-nummer til en individuell polygon (MMSI <-> polygon).
2. Fartøy av interesse liste. Her er hvert enkelt fartøy koblet til eierstruktrur (MMSI <->Eierstruktur).




Figur 7.2 Rshiny nettverksapplikasjon.

## 7.2 Modellering av nettverk

Den innledende analysen startet med geospatielle data for fartøy som har operert i norske interesseområder. I denne studien vil modelleringen av fartøy hentet ut fra AIS-databasen bli omhandlet som enheter, aktører eller noder inn i SNA. «En-mode nettverk» består av et enkelt sett aktører og relasjonene mellom dem. «To-mode nettverk» kan bestå av ulike sett aktører (for eksempel fartøyer og posisjoner) der relasjonen oppstår mellom settene og ikke internt i hvert sett (Cunningham et al., 2016, s. 46). Det er altså ingen relasjon mellom eksempelvis fartøyer isolert sett. Relasjonen oppstår ved at de eies av et moderselskap, eller stopper i samme posisjon. Oppgaven fokuserer på analyse av samtlige russiske sivile fartøyer i NØS for hele 2014 og hele 2017. Når det er sagt må man i en analyse av to-mode nettverk være påpasselig med hvordan resultatene tolkes. Everton advarer mot å trekke forhastede slutninger om tilknytning i nettverk. Bare fordi to noder, eksempelvis fartøyer, besøker samme geografiske posisjon trenger ikke nødvendigvis å bety at det er en relasjon mellom dem (Everton, 2012, s. 86).

Periodisk utsendelse i form av AIS-signaler angir posisjonering i tid og rom innenfor tidsangivelsen som denne studien omfatter. Et AIS-track er et resultat av en serie datautsendelser som i sum visuelt gjengir nodens posisjoner over tid. I denne studien knyttes det spesiell interesse til fartøyer som avviker fra normal seilingsled eller forventet seilingsmønster i norske

interesseområder. Posisjonsoppdateringer som er avgrenset til et spesifikt område over tid, og som indikerer at fartøyet har stoppet eller kadreier (manøvrere i lav hastighet) defineres til å være av spesiell interesse. Nettverksdata har blitt konstruert gjennom integrasjonen av ugraderte data hentet fra åpne databaser og bruk av algoritmer som har blitt utviklet i forbindelse med denne studien. Ut fra dette blir det mulig å generere et sosialt nettverk basert på bevegelse og nærhet mellom noder i tid og rom.

Modelleringen og algoritmene gjør det så mulig å se på enkelte enheter, hvor de har oppholdt seg, og se hvilken del av nettverket som i lys av sine bevegelser kan karakteriseres å være sentrale aktører i de respektive nettverk. Bruken av SNA kodene er fleksible. I denne oppgavens analyse er det valgt en annen tilnærming enn både studien av Odessanettverket, og studien i Sør-Kina-havet. Dette for å studere hvorvidt SNA som sådan er overførbart til norske interesseområder, og om metodene kan gi oss dypere situasjonsbevissthet i det maritime domenet. Fokuset for den metodiske tilnærmingen er å forstå mulighetene stordata og SNA gir til å kartlegge adferden til noder av interesse og deres potensielle relasjoner. Avhengig av hvilke identifikasjonskriterier man har, vil koding og algoritmer kunne tilpasses dette. Det vil også være mulig å legge på flere lag med stordata, som for eksempel bruk av sosiale medier. Verdt å merke seg er at bruken av stordata i seg selv gir begrensninger, og på grunn av sin størrelse krever forenkling. Datamengden gir utfordringer med tanke på utstyr, og har vært i grenseland for hva selv en kraftig pc klarer. Analysen er blitt gjennomført på en iMac med 3,3 GHz Intel Core i5 prosessor. Erfaring fra arbeid med datasettet viser at større prosesseringskapasitet vil være nødvendig for å analysere større spekter av stordatasettet.

For å illustrere mulighetene som ligger i bruk av stordata og SNA er det i denne oppgaven definert følgende filter for å presentere et «proof of concept» for modellering av nettverk:

- *Fartøyer* som under tilsynelatende normal transit men som i et tidsrom reduserer farten til under 1,5 knop i et område er definert som å ***kadreie***. Ved å sette dette filteret vil man avdekke stopp i de havner nodene benytter, samt hvor de eventuelt stopper opp.
- Hvis to eller flere fartøyer har kadreid, eller stoppet i samme identifiserte område defineres dette som ***samlokalisering.***
- *Selskaper* som står oppført som eier eller operatørselskap for et eller flere fartøyer som defineres som interessant.
- *Områder (Point of Interest – POI)* er områder hvor noder kadreier eller samlokaliseres gjentatte ganger. Disse vil bli geolokalisert og i seg selv opptre som noder i nettverket,

for å vurdere om ulike geografiske områder tiltrekker seg spesielle nettverksstrukturer over tid.

Med fokus på sårbarheter i norske interesseområder fokuserer oppgaven på avvikende adferd i nærheten av følgende «*point of interest*» (POI):

- Norske militære installasjoner og baser. Studien er avgrenset til objektet og de nærliggende områder til Vardø, Andøya, Ørlandet og Haakonsvern Orlogsstasjon.
- Norske olje og gassinstallasjoner, inkludert rørledninger og kommunikasjonskabler.
- Militære øvelser i 2014 og 2017. Det vil gjennomføres en komparativ analyse av de to årene for å se eventuelle sammenhenger eller utvikling.

*Fartøy av interesse (Vessel of interest-VOI)* er av alle fartøy som:

1. Regelmessig stopper/kadreier (fart <1,5 knop), i et område der det er infrastruktur og rørledninger for olje og gass næringen
2. Regelmessig stopper/kadreier (fart <1,5 knop), i et område der det befinner seg kommunikasjonskabler.
3. Regelmessig stopper/kadreier (fart <1,5 knop), i et område der det er norsk militær infrastruktur (POI).
4. Tilhører samme eierstruktur som tidligere identifiserte fartøy av interesse.
5. Regelmessig stopper/kadreier (fart <1,5 knop), i områder der det er andre fartøy av interesse som i punkt 1-4.

Gjennomgang av informasjonen i polygoner måned for måned ble registrert i en egen liste. Samtlige fartøy som gjennomførte aktivitet i henhold til kriteriene over ble registrert. Videre ble vekting av kriterier for å bli regnet som en node i en nettverksstruktur kategorisert, ved å se på antallet ganger en node gjennomførte stopp i samme område eller flere områder.

Vektingen ble gjort fra en skala fra en til fire som i figur under.

| ***Vektingskriterier*** | **Et område** | **Flere områder** |
|---|---|---|
| **Et stopp** | 1 | 3 |
| **To eller flere stopp** | 2 | 4 |

Figur 7.3 Vektingskriterier VOI – «Vessel of interest»

Algoritmene kan justeres etter behov og gjør det mulig å definere et område geografisk, for å se hvilke fartøy som passerer gjennom. Dersom man i en militær kontekst med høyere graderingsnivå og har behov for spesifikk informasjon kan analyseverktøyet kodes for å finne det man er ute etter. Dette vil ikke bli gjort i denne studien. Videre er det mulig å konstruere nettverk basert på hvilke fartøyer som i løpet av en gitt tid er samlokalisert innenfor et bestemt område. Beskrivelsen av denne studiens tilnærming til konstruksjonen av nettverk vil bli gjennomgått i neste avsnitt.

## 7.3 Nettverkspresentasjon

Analysen tar for seg nettverk bestående av fartøy, eiere, aktivitet som samlokalisering med andre fartøy i geografiske områder eller posisjoner. Disse nettverkene vil bli visualisert for vise hvilke noder som har relasjoner til andre noder, samt kunne si noe om relasjonenes styrke og nettverkenes tetthet. Presentasjonen av nettverk basert på AIS kombinert med integrasjon av fartøyenes registerdata brukes for å kunne vurdere tilknytning til eventuelle grå maritime nettverk. Med bakgrunn i fartøyets identitet, gjennom MMSI nummer eller IMO nummer ble informasjon hentet inn for hvert enkelt fartøy av interesse inkludert eierstruktur. Analysen vil ha følgende tilnærming til konstruksjon av nettverk:

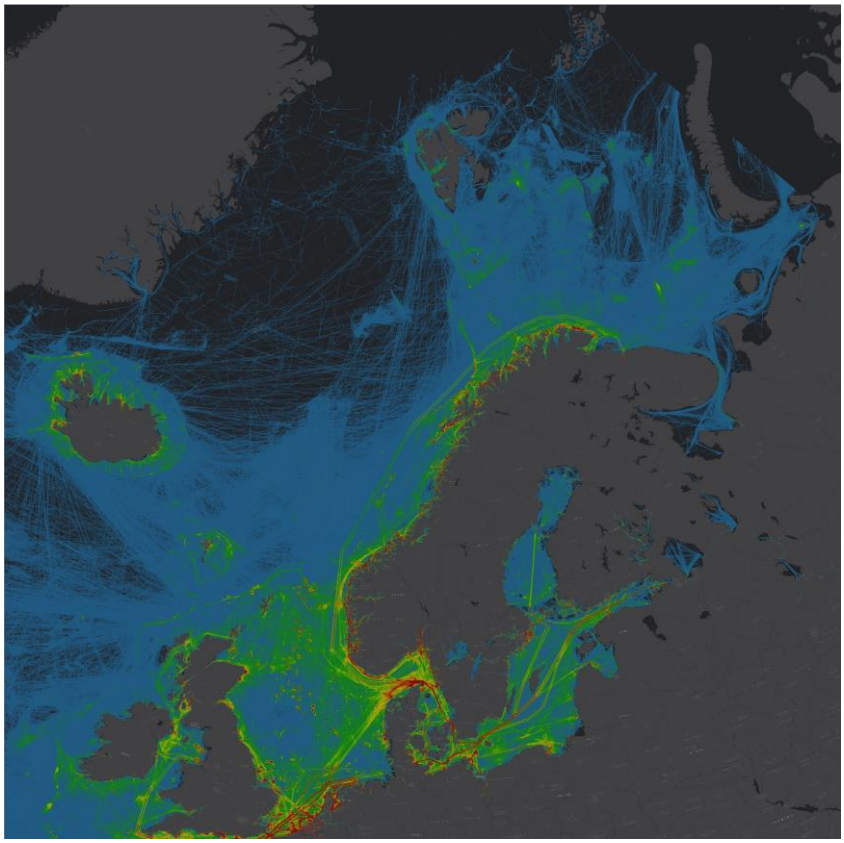
- Hvilke noder, være seg fartøy eller selskaper, utviser avvikende adferd i norske interesseområder?
- Gitt avvikende adferd, skjer dette systematisk over tid i de samme områdene?

Når MMSI nummeret er kjent fra AIS data, har nettsiden Marinetraffic.com i kombinasjon med databasene Paris Memorandum of Understanding og Lexis Nexus Advanced blitt brukt for å finne tilleggsinformasjon om fartøyer og gjort det mulig å knytte hvert enkelt fartøy til en eierstruktur. Basert på gitte kriterier ble fartøyer registrert i en «edgelist» som inneholder informasjon om relasjonen mellom nodene som i denne studien i kapittel fem ble omtalt som *ikke-retningsbestemte* (De Nooy et al., 2018, s. 7). Nettverksstrukturen ble så presentert i sosiogrammer, og relasjonene beregnet matematisk. For å illustrere hvilke relasjoner det er mellom de ulike nodene (fartøy, eierstruktur, hendelser, og aktiviteter) ble beregninger av sentralitet, tetthet, kohesjon og klynger gjennomført. Denne visualiseringen kan benyttes til å få en dypere situasjonsforståelse, samt bidra til nye perspektiver på muligheter til å studere nettverk fremfor enkeltnoder og enkelthendelser. Dette gjenspeiles i resultatene fra analysen.

# 8 Resultat og analyse

I dette kapittelet vil resultater fra stordata og fra den sosiale nettverksanalysen bli presentert. Fokuset vil være på hvordan metoder fra SNA kan benyttes for å skape en økt maritim situasjonsbevissthet, kombinert med hvordan analyse av stordata kan identifisere maritime nettverk av fartøyer og eierstruktur som potensielt kan unyttes som virkemidler i lys av russisk helhetlig tilnærming. Et representativt utvalg av resultater fra analysen av 2014 og 2017 vil bli presentert og visualisert. Eksemplene er hentet frem for å illustrere hvordan logikken fra SNA kan overføres og benyttes i det maritime domenet. Til slutt vil det bli foretatt en kvalitativ vurdering av hva resultatene fra analysen viser.

Norske interesseområder er til enhver tid tett trafikkert av fartøyer som opptrer regelmessig og i relativt faste ruter. Tettheten varierer på bakgrunn av etterspørsel av last, reguleringer i fiskerinæringen, sesong (vær og vind), og aktivitet tilknyttet olje og gassindustrien.



Figur 8.1 AIS tetthetsplott norske interesseområder 2017 (FFI v/Morten Aronsen)

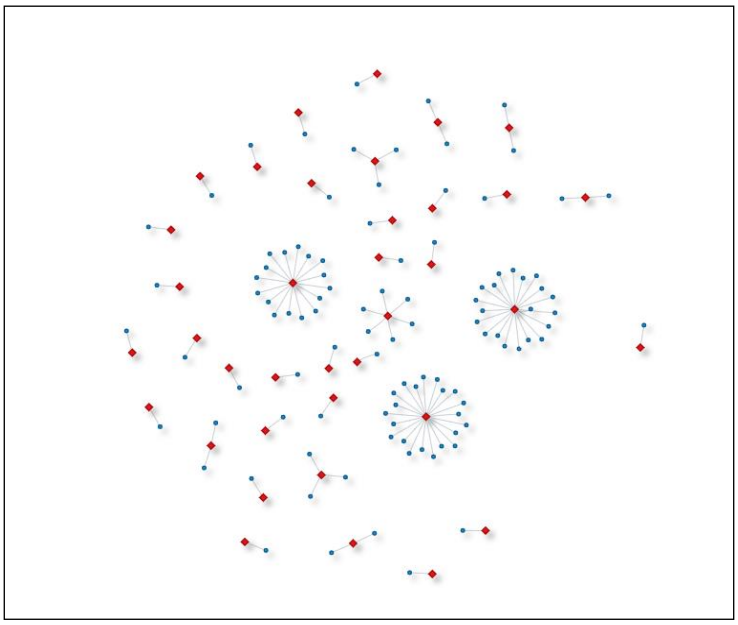
Mye av observert russisk aktivitet i norske interesseområder er knyttet til fiskerier og varierer således med årstid. Variasjonen i observert fiskeriaktivtet, inkludert den russiske, i den perioden vi har analysert AIS data (2014 og 2017) anses ikke å være unormal. Fiskefartøyer som

bedriver fiske eller som er registrert til kai i norske havner knyttet til verfts- eller fiskeriindustri vil derfor i utgangspunktet ikke bli omfattet av studien. Basert på anbefalinger fra Dr. Wayne Porter ved NPS, som ledet US Navy sin maritime nettverksstudie i Sør-Kina-havet, er allikevel noen fiskefartøyer inkludert i datagrunnlaget for å vise at disse utgjør en faktor man ikke kan se bort fra.

# 8.1 Maritim nettverksanalyse 2014.


Figur 8.2 Visualisering fartøyer med fart <1,5 knop - januar 2014. Bildet er generert som et resultat av koding (T-Locoh) og sammenkobling av kartinformasjon (Leaflet) ved bruk av programmeringsspråket R.

Figur 8.2 viser samtlige russiske fartøy som gjennom i januar 2014 har hatt stopp eller som er registrert med en fart mindre enn 1,5 knop.



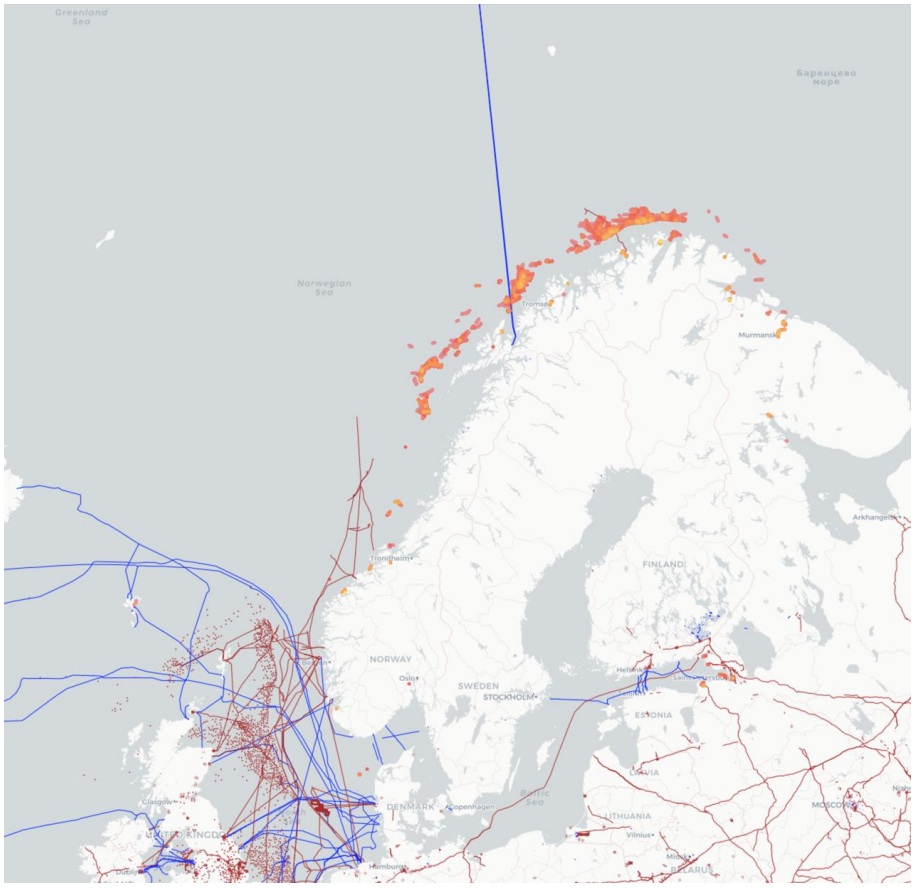
Figur 8.3 Initiell visualisering av fartøyer (blå noder) og eierstruktur (røde noder) 2014

I snitt er 8000 fartøyer uavhengig av nasjonalitet eller flaggstat observert i 2014. Gitt oppgavens definerte kriterier[9] for hva som utgjør et fartøy av interesse, har analysen identifisert 126 russiske fartøyer. Av disse ble 12 fartøyer vektet til kategori 4[10], ved at de flere ganger i løpet av perioden stoppet i flere områder. Disse fartøyene har en eierstruktur bestående av 34 selskaper, inkludert fartøyer direkte eller indirekte eid av Den Russiske Føderasjon. Figur 8.3 er et eksempel på en visuell fremstilling av dette. De røde nodene er selskaper, mens de blå representerer fartøyer.

Mange av de samme fartøyene gjennomfører gjentatte stopp flere steder langs kysten. Dette skjer i områder som ikke vurderes som sentral i utførelsen av primæroppgaven, som i de fleste tilfeller er å frakte gods fra A til B. Dette gjelder Barentshavet i tilknytning til Vardø, tilstøtende områder til Andøya, Frohavet ved Ørlandet flystasjon, i havet i de tilstøtende områdene rundt Bergen, samt Stavanger med tilhørende oljeindustri. Fartøy fra ulike selskaper utviser avvikende aktivitet i samme område, noe som kan indikere at de kan ha sammenfallende interesser. I 2014 registreres det høy nettverksaktivitet fra blant andre selskapene *Northern Shipping Company (NSC), Murmansk Shipping Company (MSC),* og det statseide *Sovcomflot (SCF).* Direktøren i Sovcomflot var russisk transportminister i perioden 1998 til 2004. Videre knyttes det også interessante funn til blant andre selskapene *FEMCO* og *North-Western Shipping Company (NWSC).* Disse selskapene omtales også i rapporten *«The Odessa Network»* blant aktørene som i det russiske systemet har bidratt til våpeneksport til blant annet Syria (Wallace &

[9] Se avsnitt 7.2 «Modellering av nettverk»
[10] Kategori 4 – To eller flere stopp i flere områder.

Mesko, 2013, s. 59). Fartøyene «Alaed» (MMSI 273355170) og «*Professor Katsman*» (273355040), som tilhører de respektive selskapene over, har blitt brukt til sensitive leveranser på vegne av den russiske staten. Begge fartøyene er i analysen blitt registrert aktive i våre interesseområder gjennom 2014.




Figur 8.4 Statistiske data mars 2014. Bildet er generert som et resultat av koding (T-Locoh) og sammenkobling av kartinformasjon (Leaflet) ved bruk av programmeringsspråket R. Rørledninger til olje og gass er vist som røde streker, mens kommunikasjonskabler er vist som blå streker. Fargen på polygon indikerer tetthet på registrerte AIS data.

For å komme frem til det overordnede resultatet har det vært nødvendig å utforske datagrunnlaget måned for måned. Figur 8.4 er et eksempel. Figuren viser registrerte AIS data for russiske fartøy for mars 2014. Disse har i et gitt område operert med en fart på mindre enn 1,5 knop. Hver enkelt polygon blir visuelt fremstilt på bakgrunn av AIS informasjonen, kodet og beregnet ved bruk av filter og algoritmer benyttet i R. For å illustrere hvordan datasettet er benyttet for å bygge opp nettverksmodellene blir dette vist i følgende eksempel. Tabellene under viser to matriser for rådata som AIS informasjonen gir. Avgrensningen som i oppgaven er benyttet som definisjon på «fartøy av interesse» er brukt for å demonstrere hvordan man ved bruk av filter i kodingen kan se etter spesifikke data. Samtlige fartøyer som tilfredsstiller dette kriteriet vil grunnet kodingen av algoritmene bli presentert i en egen liste, og posisjonen vil bli identifisert som en polygon på kartet. Dette polygonet vises med koden id_iso_XX_XX

(eksempel fra figur 8.5 under id_iso 50_48). Hver enkel polygon fremstilles med en fargekode som indikerer tettheten på AIS utsendelser som er registrert. Tetthet gjenspeiler antall AIS registreringer for en spesifikk node i et område. Høyest tetthet på antallet AIS registreringer innenfor et gitt område visualiserers ved røde, oransje eller gule polygon. Gule polygon representerer de deler av det totale området hvor det er størst geospatiell tetthet på målingene (flest registrerte AIS-registreringer innenfor 10% av de områdene hvor fart er målt lavere enn 1,5 knop). Denne oppgaven har ikke differensiert med tanke på tetthet, men kartlagt alle fartøyer i henhold til modelleringskriterier gitt i kapittel 7.

Tabellene 8.1 og 8.2 er data fra mars 2014 og illustrerer et avvik fra normalsituasjonen i samme periode og samme område som øvelse Cold Response pågikk.

| MMSI | DTG | Lengde | Bredde | SOG | COG | True head |
|---|---|---|---|---|---|---|
| 273338310 | 13.03.2014 00:16 | 16,0913 | 69,0819 | 12 | 241,2 | 240 |
| 273338310 | 13.03.2014 00:24 | 16,04 | 69,0699 | 8,1 | 231,5 | 226 |
| 273338310 | 13.03.2014 00:25 | 16,0354 | 69,0684 | 7,9 | 225,8 | 221 |
| 273338310 | 13.03.2014 00:32 | 16,0121 | 69,0582 | 7,5 | 217,3 | 214 |
| 273338310 | 13.03.2014 00:39 | 15,9881 | 69,0466 | 5,7 | 216,5 | 214 |
| 273338310 | 13.03.2014 00:41 | 15,984 | 69,0446 | 5,1 | 216,4 | 215 |
| 273338310 | 13.03.2014 00:48 | 15,9705 | 69,038 | 2,5 | 212,4 | 223 |
| 273338310 | 13.03.2014 00:51 | 15,9691 | 69,0371 | 0,6 | 200,1 | 252 |
| 273338310 | 13.03.2014 00:55 | 15,9708 | 69,0368 | 0,5 | 93,7 | 270 |
| 273338310 | 13.03.2014 01:04 | 15,9734 | 69,0366 | 0,1 | 100,9 | 274 |
| 273338310 | 13.03.2014 01:07 | 15,973 | 69,0366 | 0,3 | 274,6 | 273 |
| 273338310 | 13.03.2014 01:13 | 15,9716 | 69,0368 | 0,3 | 284,5 | 275 |

Tabell 8.1 AIS-informasjon for «*Zapolyare*» (MMSI 273338310)[11]

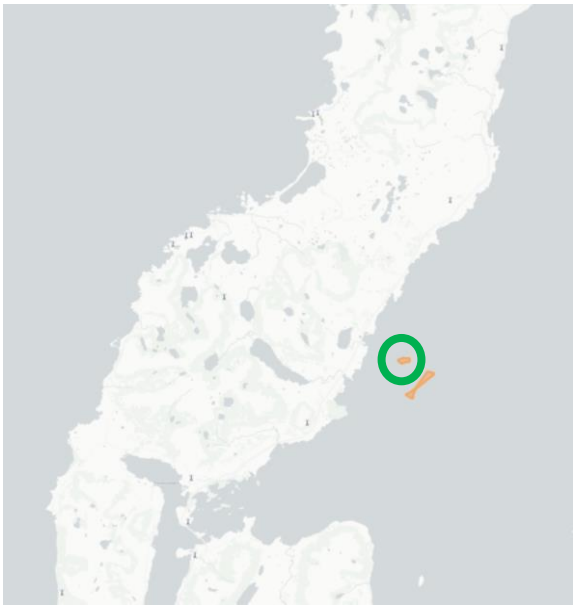
Figur 8.5 Visualisering «Zapolyare» markert med grønn sirkel

Tabell 8.1 og 8.2 illustrerer begge informasjon fra AIS, og må sees i sammenheng med henholdsvis figur 8.5 og 8.6. som representerer en grafisk fremstilling av samme data. De to fartøyene i eksempelet under var samlokalisert i Andfjorden på samme tidspunkt.

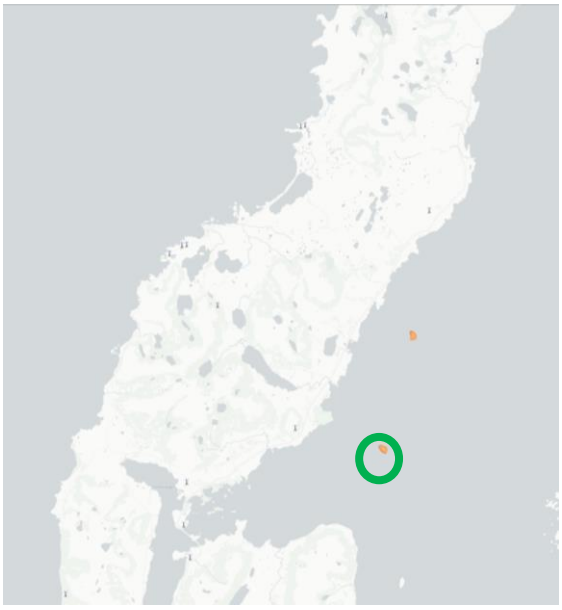
[11] Se kapittel 5.1

| MMSI | DTG | Lengde | Bredde | SOG | COG | True head |
|---|---|---|---|---|---|---|
| 273118000 | 13.03.2014 00:04 | 15,9546 | 69,0571 | 0,1 | 218,3 | 170 |
| 273118000 | 13.03.2014 00:07 | 15,9546 | 69,0571 | 0,1 | 218,3 | 167 |
| 273118000 | 13.03.2014 00:10 | 15,9545 | 69,0571 | 0,1 | 218,3 | 165 |
| 273118000 | 13.03.2014 00:16 | 15,9542 | 69,057 | 0,1 | 254,2 | 155 |
| 273118000 | 13.03.2014 00:22 | 15,954 | 69,057 | 0,1 | 255,4 | 146 |
| 273118000 | 13.03.2014 00:28 | 15,9539 | 69,057 | 0,1 | 224,2 | 137 |
| 273118000 | 13.03.2014 00:34 | 15,9537 | 69,0569 | 0,1 | 247,5 | 127 |
| 273118000 | 13.03.2014 00:37 | 15,9536 | 69,0568 | 0,1 | 227,9 | 125 |
| 273118000 | 13.03.2014 00:43 | 15,9536 | 69,0568 | 0,1 | 281,2 | 123 |
| 273118000 | 13.03.2014 00:46 | 15,9536 | 69,0568 | 0,1 | 281,2 | 118 |
| 273118000 | 13.03.2014 00:52 | 15,9535 | 69,0567 | 0,1 | 281,2 | 110 |
| 273118000 | 13.03.2014 00:58 | 15,9534 | 69,0566 | 0,1 | 281,2 | 99 |

Tabell 8.2 AIS informasjon for «Mekhanik Pyatlin» (MMSI 273118000)[12]



Figur 8.6 «Mekhanik Pyatlin» (MMSI 273338310) mars 2014



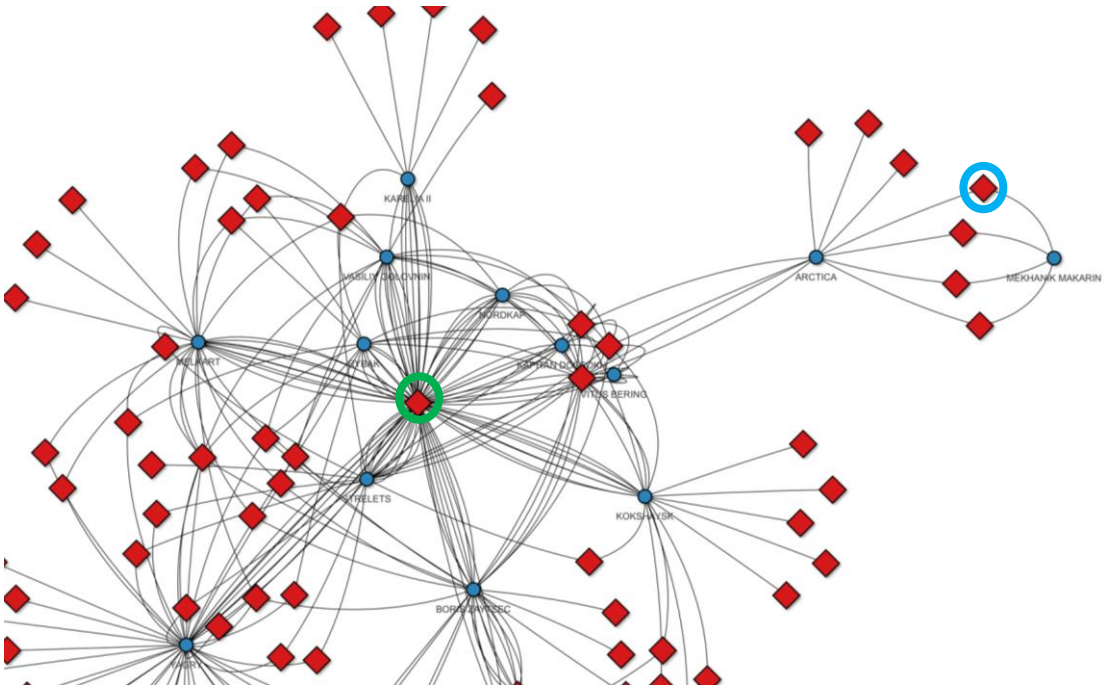
Figur 8.7 «Alaed» (MMSI 273355170) september 2014

Videre viser figur 8.7 hvor *«Alaed»* (MMSI 273355170) stoppet i Andfjorden september 2014. Tre unike noder fra tre ulike selskaper har oppholdt seg i samme område, hvorav to av dem (figur 8.5 og 8.6) samtidig. Totalt 7 fartøyer gjennomførte slike stopp dette området i 2014. En av forklaringene på dette kan være så enkelt som at fartøyene har ligget værfast og har søkt såkalt «shelter» før de går videre. Dette gjør at det på tross av at metoden kan gi oss en økt situasjonsbevissthet, fremdeles er utfordrende å skille de uskyldige hendelsene fra de som ikke er det. Eksemplet representerer allikevel et lite utvalg fra datasettet, men illustrerer hvordan

[12] Se kapittel 5.1

metoden kan anvendes for å danne grunnlag for analyse av maritime nettverksstrukturer ved bruk av SNA. Dette eksempelet illustrerer også hvordan analysen har forholdt seg til begrepet *fartøy- og område av interesse*. Der det ble registrert avvik, ble prosessen gjennomført iterativt. Slik får man klarhet i om det finnes andre sammenhenger gjennom året eller mellom årene. Når slike hendelser er gjentagende er det naturlig å også se på andre fartøyer tilknyttet samme eierstruktur. En rekke av de identifiserte fartøyene utviser regelmessige «uregelmessigheter». Avvikende adferd skjer regelmessig i samme områder, og det er et mønster i hvilke selskaper som sitter på eiersiden.

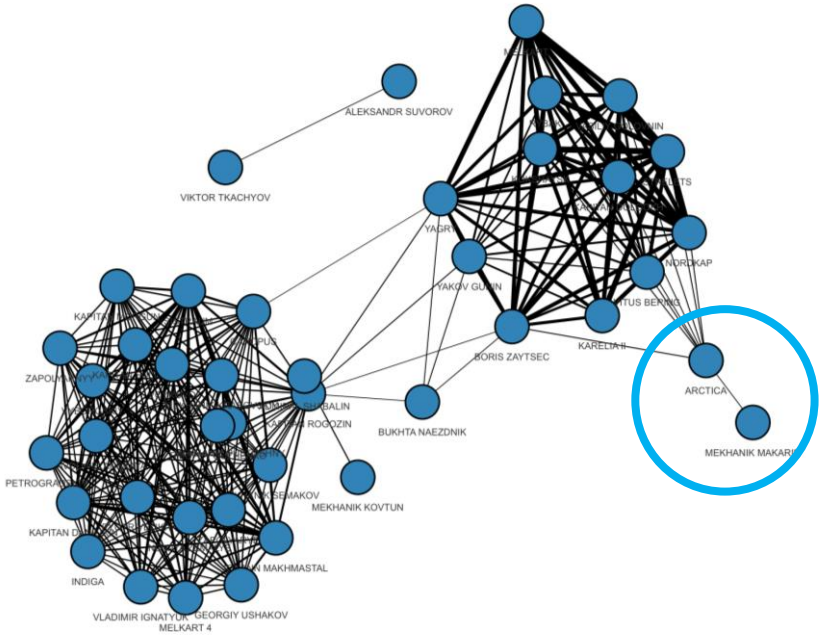
For ***januar*** 2014 gir analysen et forventet bilde av omfattende trafikk og fiskeriaktivitet. Figur 8.8 er en visuell fremstilling av et nettverk. Dette sosiogrammet fremstiller en graf som viser noder, og deres relasjoner (kanter).



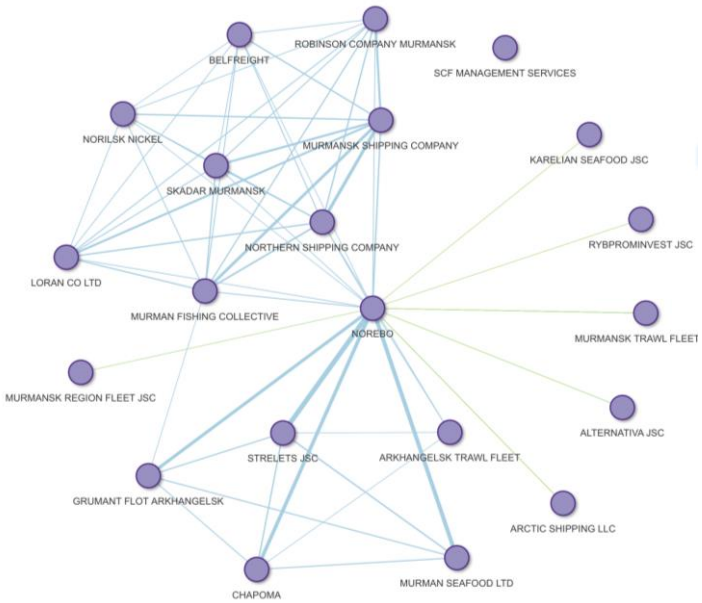

Figur 8.8 Aktivitet med utgangspunkt i Tromsøflaket (grønn sirkel) – og nettverkets utstrekning til Bergen (blå sirkel) januar 2014. Blå noder er fartøyer. Røde firkanter er fartøyers stoppunkter.

Tettheten for fartøyers samlokalisering påvirkes av at de for eksempel er registrert til kai eller er samlokaliserte i annen aktivitet i samme område. Mange av fartøyene i studien har for Murmansk som hjemmehavn, eller leverer fisk i eksempelvis Kirkenes eller Tromsø. Slike registreringer vil påvirke den beregnede nettverkstettheten. Disse faktorene vil kunne gi utslag som påvirker resultatene i den påfølgende maritime nettverksanalysen. Dette er av stor viktighet for vurdering av resultatene, fordi det da kan fremstå som om nettverkene har stor tetthet, eller at

sentralitet i nettverk er forårsaket av bevisst samlokalisering, mens det i realiteten er andre faktorer eller tilfeldigheter som avgjør.

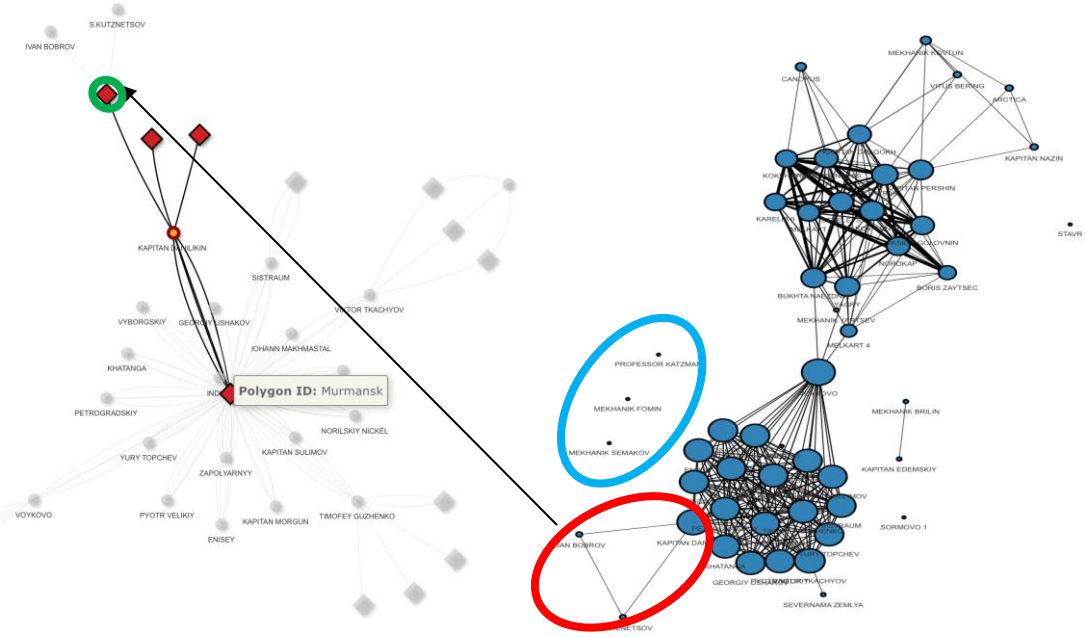



Figur 8.9 Samlokalisering fartøyer januar 2014. Jo tykkere kanter mellom noder indikerer større grad av samlokalisering. Relasjonen mellom noder knyttet til Bergen i figur 8.8 vises her med blå sirkel.




Figur 8.10 Visualisering «to-mode» nettverk, og viser eierstruktur januar 2014. Blå streker er resultat av samlokalisering selskapenes fartøyer. Tykkere streker markerer større tetthet i form av flere registrerte samlokaliseringer. Grønne streker representerer en forretningsmessig forbindelse. I dette eksempelet er dette datterselskaper av fiskerikonglomeratet Norebo.

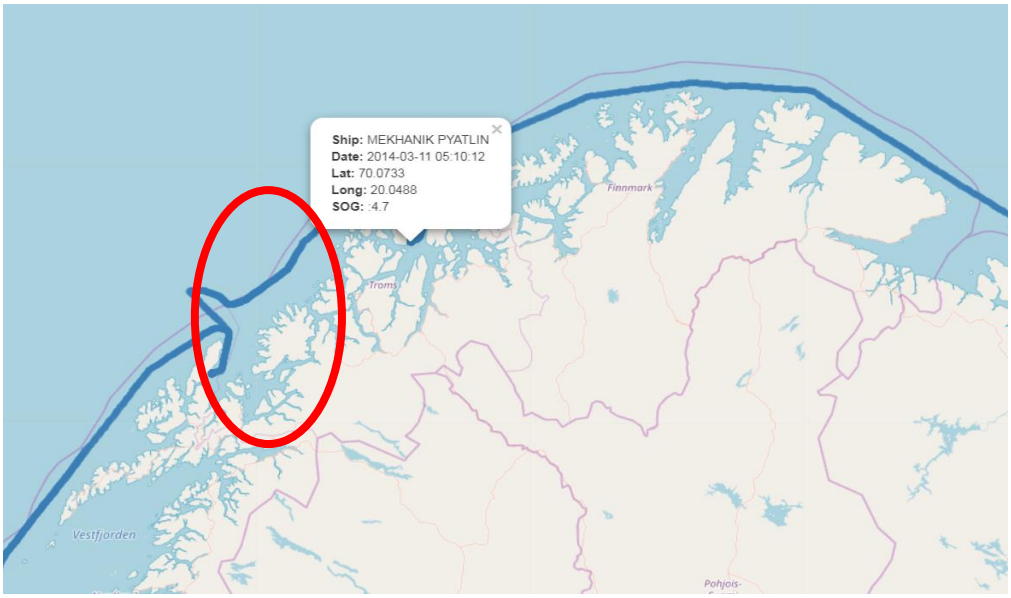
I ***februar*** er det identifisert uregelmessigheter i samme tidsrom som det årlige ubåtsjefskurset ble arrangert i regi av Sjøforsvaret i havområdene rundt Bergen (Forsvaret, 2015b, s. 100). Dette er en aktivitet som også tiltrekker seg allierte NATO partnere. I 2014 ble kurset gjennomført fra 2. februar til 13. februar. *«Mekhanik Fomin»* passerer Grimstadfjorden og Haakonsvern Orlogsstasjon på vei nordover 3. februar klokken 11:16. Senere, i perioden 22. – 24. februar, ligger *«Mekhanik Fomin»* i ro i Bjørnafjorden. Bjørnafjorden er et mye brukt øvelsesområde for Sjøforsvaret. Det antas at fartøyet var oppankret på dette tidspunktet. Et annet funn er *«Professor Katsman»* (MMSI 27355040) som var fortøyd i Fredrikstad havn 8. -10. februar. Eierselskapet *Nortwestern-Shipping Company* er igjen eid av *Universal Cargo Logistics (UCL)* som er eid av den russiske ogliarken Vladimir Lisin (Wallace & Mesko, 2013, s. 46). Eksemplene over er enkeltfunn basert på historiske data. Figur 8.11 illustrerer muligheten man gjennom maritim nettverksanalyse har til å knytte fartøyer av interesse til hverandre, til havner, samt skape en dypere forståelse av samlokalisering i særskilte områder av interesse. Nettverket på venstre side viser fartøyer og polygoner for kadreiing med fart <1,5 knop. *«Kapitan Danilikin»* (MMSI 273131200) har vært samlokalisert med to andre fartøyer i Nordsjøen. Nettverket på høyre side illustrerer i hvilken grad fartøyer har vært samlokalisert med hverandre. Den registrerte samlokaliseringen finner vi igjen til høyre, markert med rød ring. Tykkelsen på *kanten* viser i hvilken grad nodene har vært samlokalisert flere ganger. Tettheten i nettverket er blant annet et resultat av fiskeriktivitet i fiskefeltene fra Røstplatået til Nordkappbanken.




Figur 8.11 Sammenhenger i nettverk basert på to grafiske fremstillinger basert på data fra 2014. Venstre side viser fartøy (sirkler) og stoppunkter (firkanter). Høyre side viser samlokalisering av fartøyer (blå noder). Størrelse på noder reflekterer gradssentralitet. Jo større noder jo flere kanter eller relasjoner har de. Rød ring markerer hvordan man kan se disse i en sammenheng med

fartøysnettverket til venstre (Nordsjøen markert med grønn ring). Blå sirkel markerer enkeltfunn hvor samlokalisering ikke har skjedd.

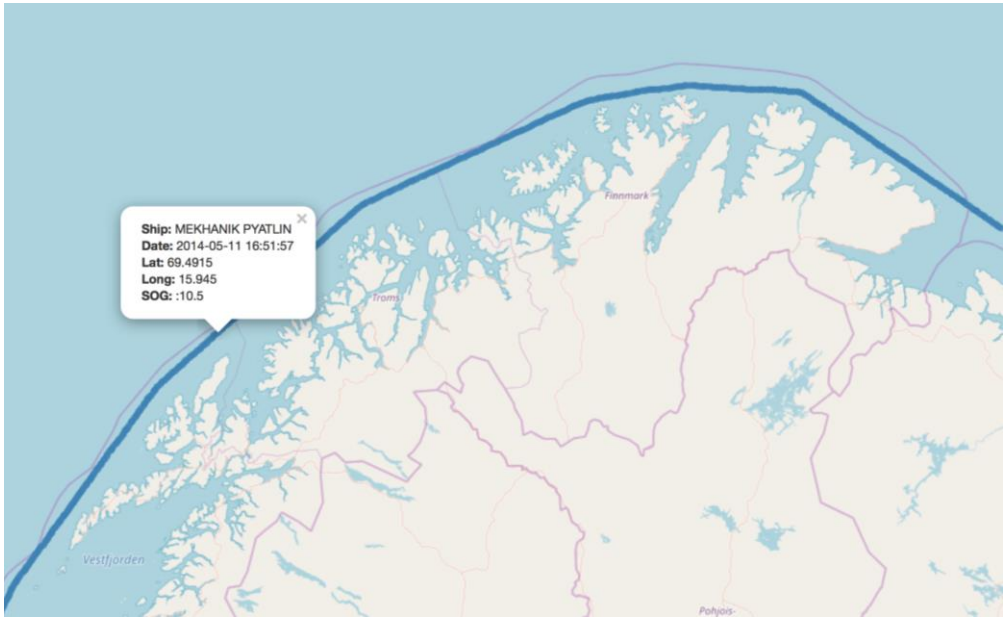
I ***mars*** ble øvelsen Cold Response 2014 gjennomført. Øvelsen pågikk i området Nordland-Troms i tidsrommet 7. – 21. mars. Figur 8.12 og 8.13 viser trackhistorikken til *«Mekhanik Pyatlin»* (MMSI 273338310) den 7. mars til 15. mars 2014. Fartøyet stopper først syd av Vanna i Troms hvor den oppholder seg i perioden 8. – 11. mars. *«Pyatlin»* går så videre Andfjorden i perioden 12. – 15. mars før det fortsetter seilas sydover.



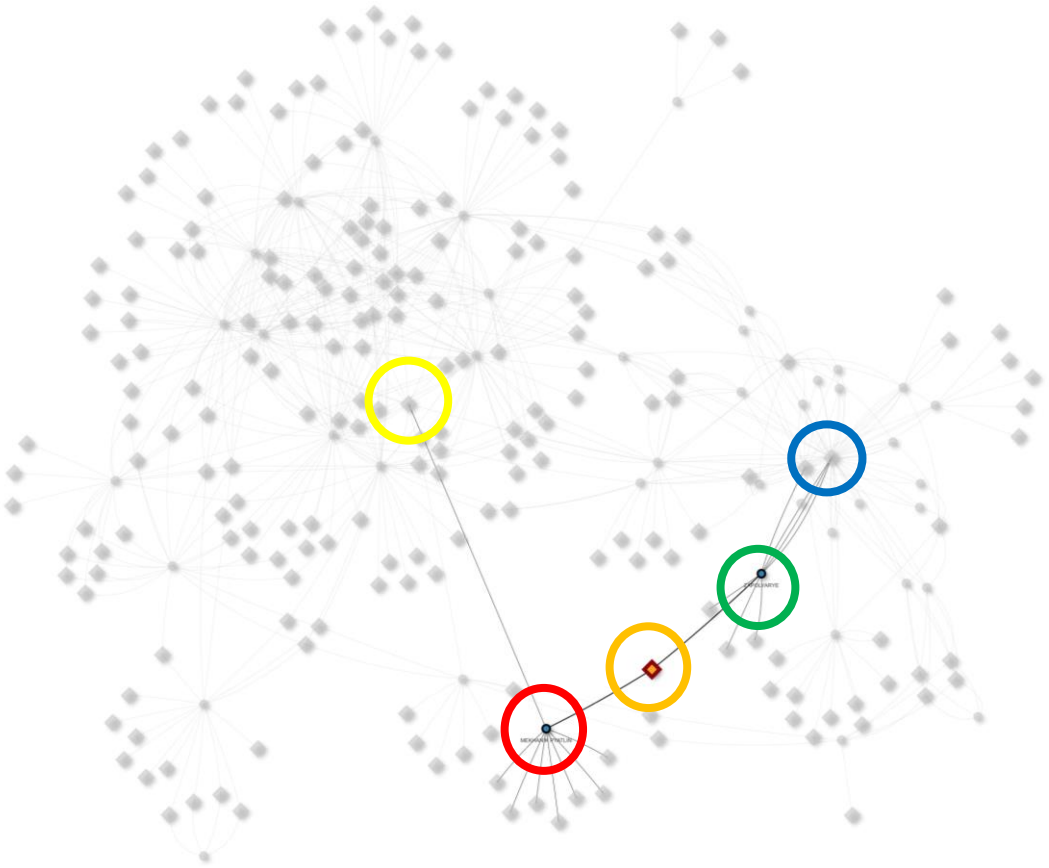

Figur 8.12 «Mekhanik Pyatlin» 11. mars 2014


Figur 8.13 «Mekhanik Pyatlin» 12. mars 2014

Figur 8.14 viser trackhistorikken for samme fartøy 11. mai, i en periode det ikke er øvelse i området. Eksemplene er tatt med for å illustrere hvordan bruk av stordata og SNA kan bidra til å se avvik i sammenheng, og hvordan analyse av samlokalisering kan bida til å avdekke andre interessante aspekter ved de maritime nettverkene.

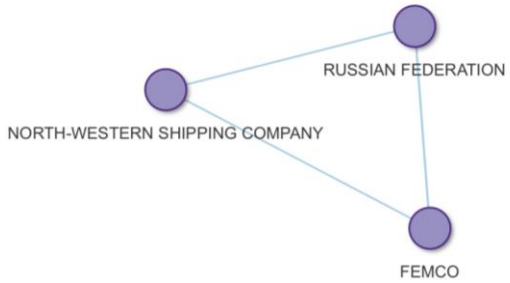



Figur 8.14 «Mekhanik Pyatlin» 11. mai 2014



Figur 8.15 Nettverk med utgangspunkt i Andfjorden (oransje sirkel) mars 2014. Nettverkets firkanter illustrerer stoppunkter - fart <1,5knop. *Gul sirkel* markerer bankene utenfor Troms. *Rød sirkel* markerer «Mekhanik Pyatlin», *grønn sirkel* markerer «Zapolyare», *blå sirkel* markerer Murmansk.

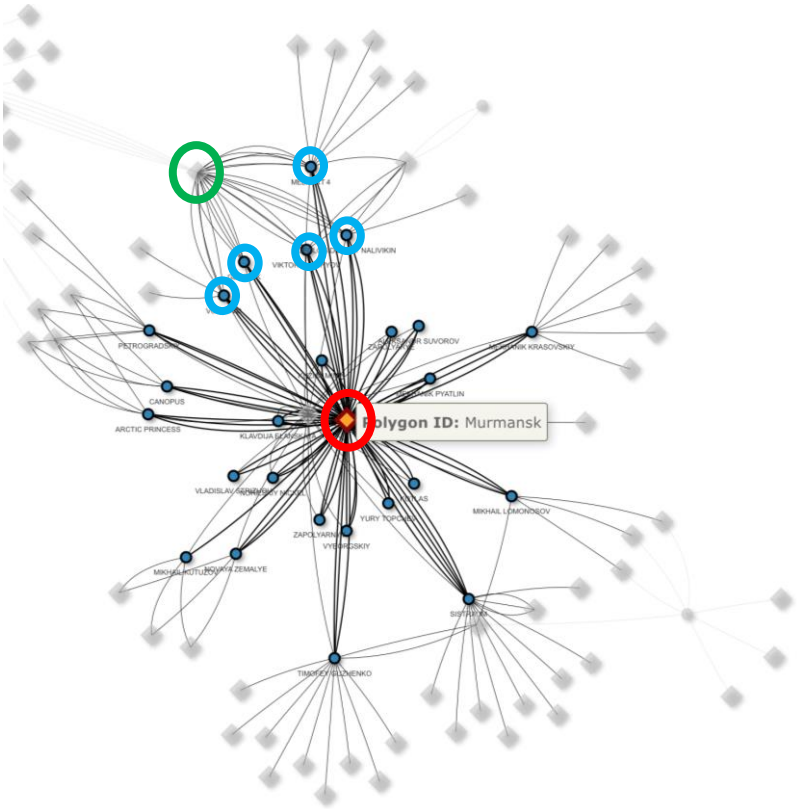
Figur 8.15 viser nettverksforbindelser fra to fartøy av interesse til andre fartøy det er mulig å knytte til nettverket samt andre områder av interesse. *«Mekhanik Pyatlin»* knyttes her til Andfjorden og *«Zapolyare»*, Murmansk, fiskebankene utenfor Troms samt andre noder i nettverkene som befinner seg på de lokasjonene. Samme måned kadreier *«Mekhanik Pustoshnyy»* (MMSI 217114000) på Frohavet ved Ørland Flystasjon og «*Mekhanik Kraskovskiy»* (MMSI 273116000) i Norskehavet vest av Ålesund. Avvikene er knyttet til samme eier, NSC. Ved å benytte SNA til å studere samlokalisering av *selskaper* basert på fartøyers adferd kan man også identifisere nettverksstrukturer.



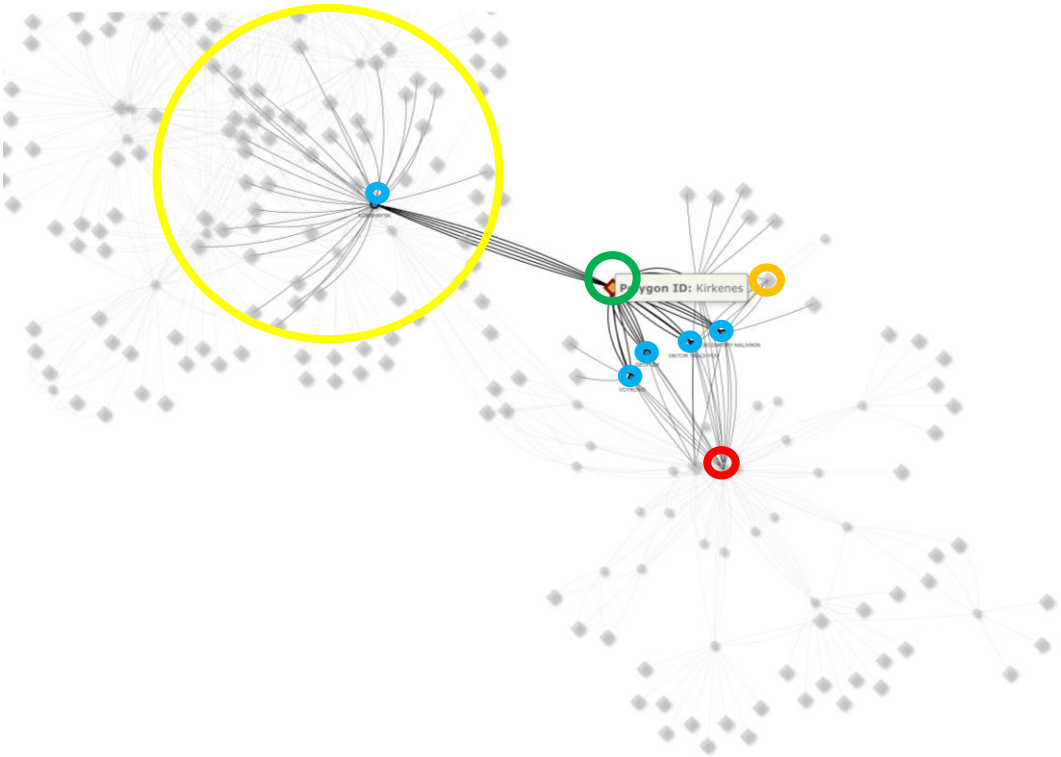

Figur 8.16 Illustrasjon på (to-mode nettverk) ulike aktørers samlokalisering mars 2014

Som et eksempel på dette befant de tre fartøyene *«Alaed»* (MMSI 273355170), *«Agate»* (MMSI 273333440), og *«Kapitan Dranitsyn»* (MMSI 273138300) seg i perioden i St. Petersburg. *«Alaed»*og «*Agate»* er eid av henholdsvis North-Western Shipping Company og FEMCO. Sistnevnte er en russisk statseid isbryter. Figur 8.16 illustrerer dette.

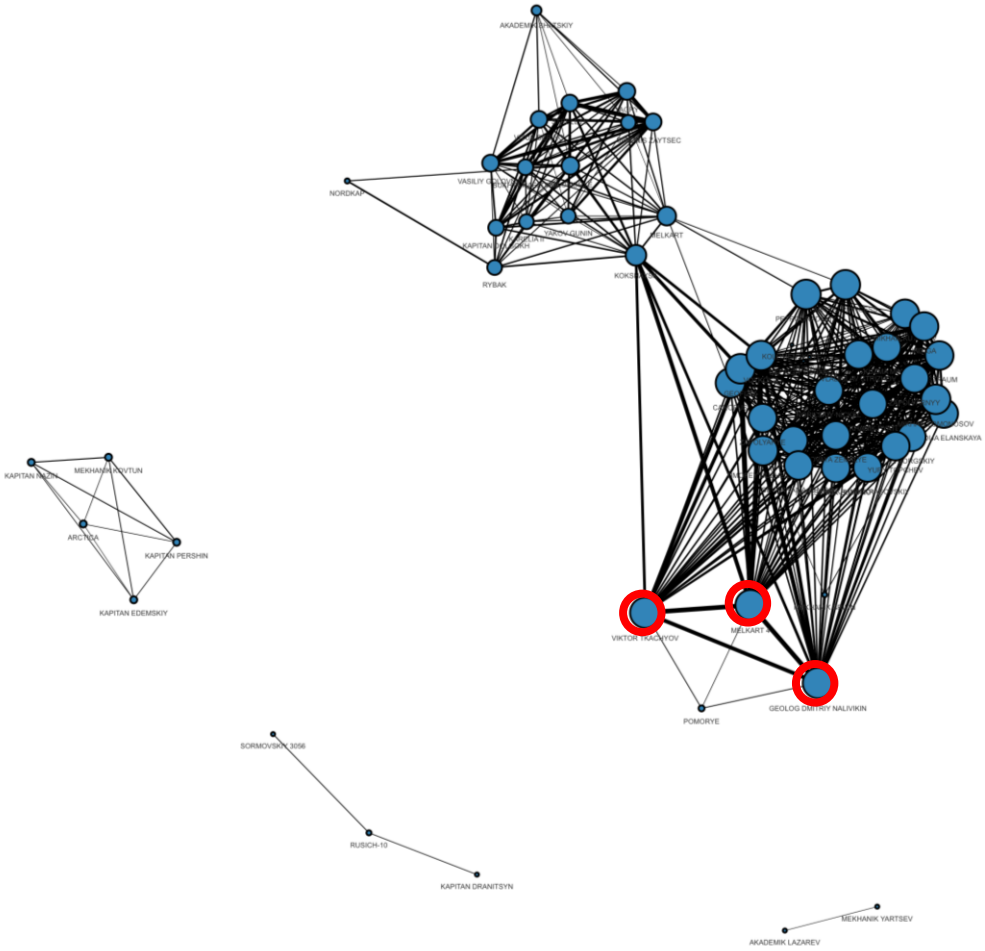
***I april*** registreres russisk seismikkaktivitet både i Barentshavet og Nordsjøen. Denne aktiviteten er også å karakterisere som en normalsituasjon, men hvor man finner russisk statlig eierskap over fartøyer og holdingselskaper. Av andre fartøy som registreres i Nordsjøen eller Skagerrak er 50% av disse fartøyene eid av Northern Shipping Company. Et annet funn er *«Rusich 5»* (MMSI 273317430) til kai i Fredrikstad. Også dette fartøyet eies av North-Western Shipping Company med sin tidligere omtalte tilknytning til *Odessanettverket*. Modelleringen av nettverkene under (figur 8.17-8.18) illustrerer hvordan ved å følge *kantene* i et nettverk kan studere relasjonene eller *stiene* mellom ulike noder *(Cunningham et al., 2016, s. 403)*.




Figur 8.17 Illustrasjon. Man tar utgangspunkt i Murmansk (rød sirkel) og identifiserer noder (blå sirkler) som også har kanter tilknyttet Kirkenes (grønn sirkel).



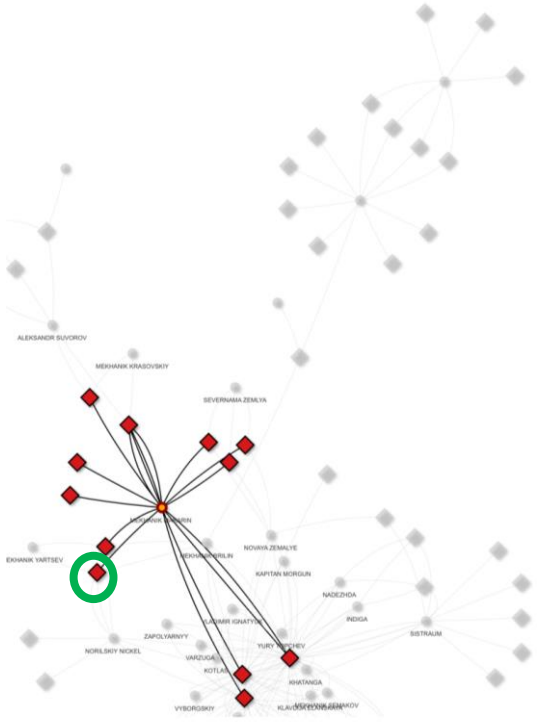

Figur 8.18 Man tar utgangspunkt i Kirkenes (grønn sirkel) og identifiserer noder (blå sirkler) som også har kanter tilknyttet andre klynger (fiskeriaktivitet fra Nordbanken til Vesterålen (markert med gul sirkel), eller området Østbanken øst av Vardø (markert ved oransje sirkel)




Figur 8.19 Samlokalisering av maritime nettverk. Rød sirkel markerer fartøyene med høyest gradssentralitet, «Viktor Tkachyov», «Geolog Dmitriy Nalivikin» og fiskefartøyet «Melkart 4» har alle like mange kanter knyttet til seg. I dette eksempelet er antallet kanter for alle de tre fartøyene 28. Gradssentralitet er et mål på hvor mange forbindelser en spesifikk node har, og kan være et måleparameter på aktivitet. I dette eksempelet tolkes resultatet til å ha blitt påvirket av grad av samlokalisering med andre fartøy i blant annet Murmansk. Dette kan bidra til unøyaktige målinger.

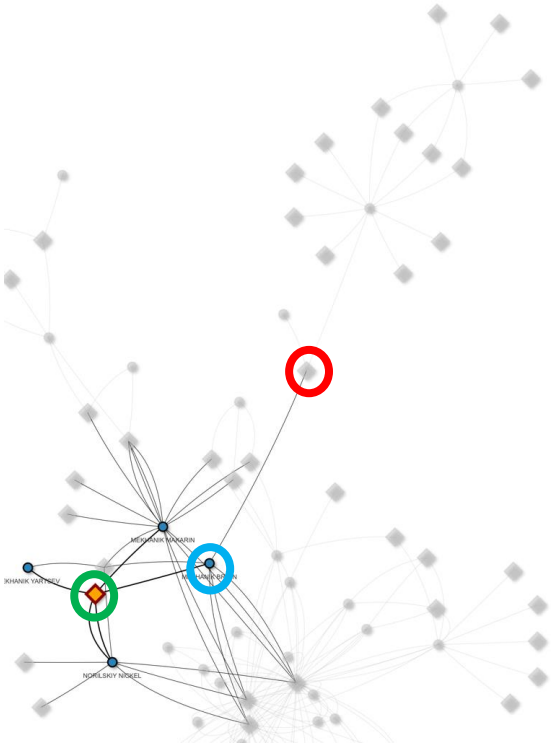
Analysen av ***Mai*** måned viser at aktiviteten til fartøyer tilknyttet selskapene *NSC* og *MSC* øker og virker mer synkronisert. Vektingen av enkelte VOI, som *«Mekhanik Makarin»* (MMSI 273115700) og *«Mekhanik Pustoshnyy»* (MMSI 273114000), når kategori 4 (stopp i en rekke områder-en rekke ganger). Dette kan indikere et mønster. Figur 8.20 til 8.23 illustrerer hvordan man sekvensielt kan utforske stier og relasjoner i maritime nettverk.

Figur 8.20 representerer en inngangsverdi. I dette eksempelet er valgt fartøy av interesse, *«Mekhanik Makarin»*.



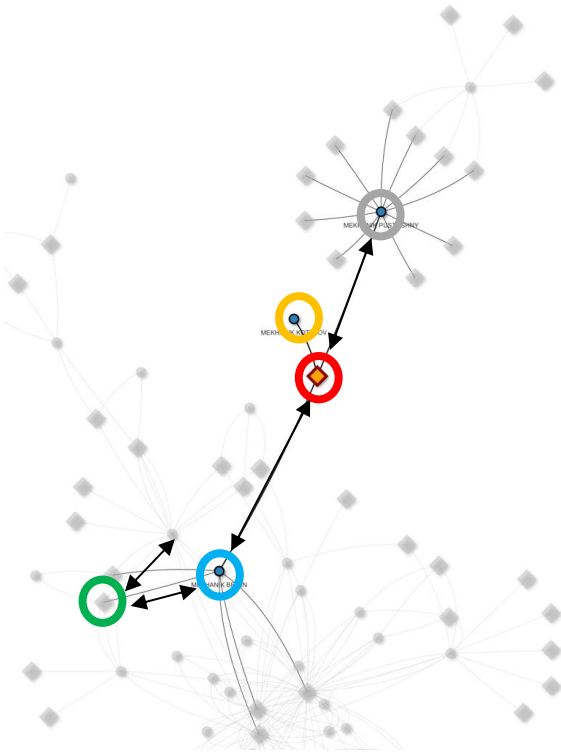

Figur 8.20 «Mekhanik Makarin» er benyttet som utgangspunkt. Relasjon til Østbanken ved Vardø markert med grønn sirkel.

Figur 8.21 representerer et område av interesse, i dette eksempelet Østbanken utenfor Vardø som *«Mekhanik Makarin»* har besøkt. Analysen viser at et nettverk bestående av fire fartøyer har besøkt samme område.



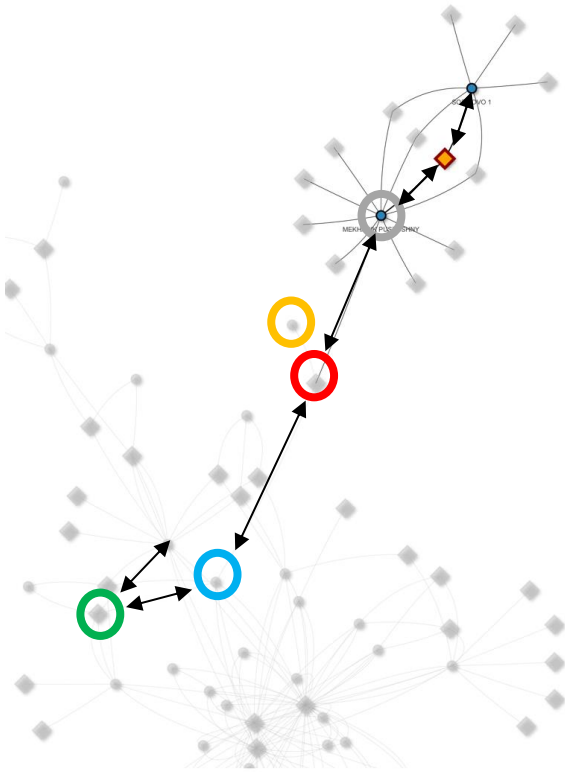
Figur 8.21 Østbanken ved Vardø markert med grønn sirkel. «Mekhanik Brilin» markert med blå sirkel. Stoppunkt for «Mekhanik Brilin» på Trøndelagskysten markert med rød sirkel.

Figur 8.22 illustrerer hvordan man kan se sammenhenger ved å følge *kantene* eller *stien* videre. Figuren viser relasjonen mellom tre fartøyer fra NSC som gjennomførte stopp i området havet vest av Ytter-Vikna på Trøndelagskysten i perioden når øvelse Trial Unified Vision 2014 ble gjennomført på Ørlandet. Atten NATO medlemsland og 2000 deltakere bidro i denne øvelsen som var den største testen av NATO Joint intelligence, surveillance and reconnaissance (JISR) (NATO, 2014a).



Figur 8.22 Østbanken ved Vardø markert med grønn sirkel. «Mekhanik Brilin» markert med blå sirkel. Stoppunkt for «Mekhanik Brilin» på Trøndelagskysten markert med rød sirkel. «Mekhanik Kottsov» (oransje sirkel) og «Mekhanik Pustoshnyy» (grå sirkel) har stoppet i samme område.

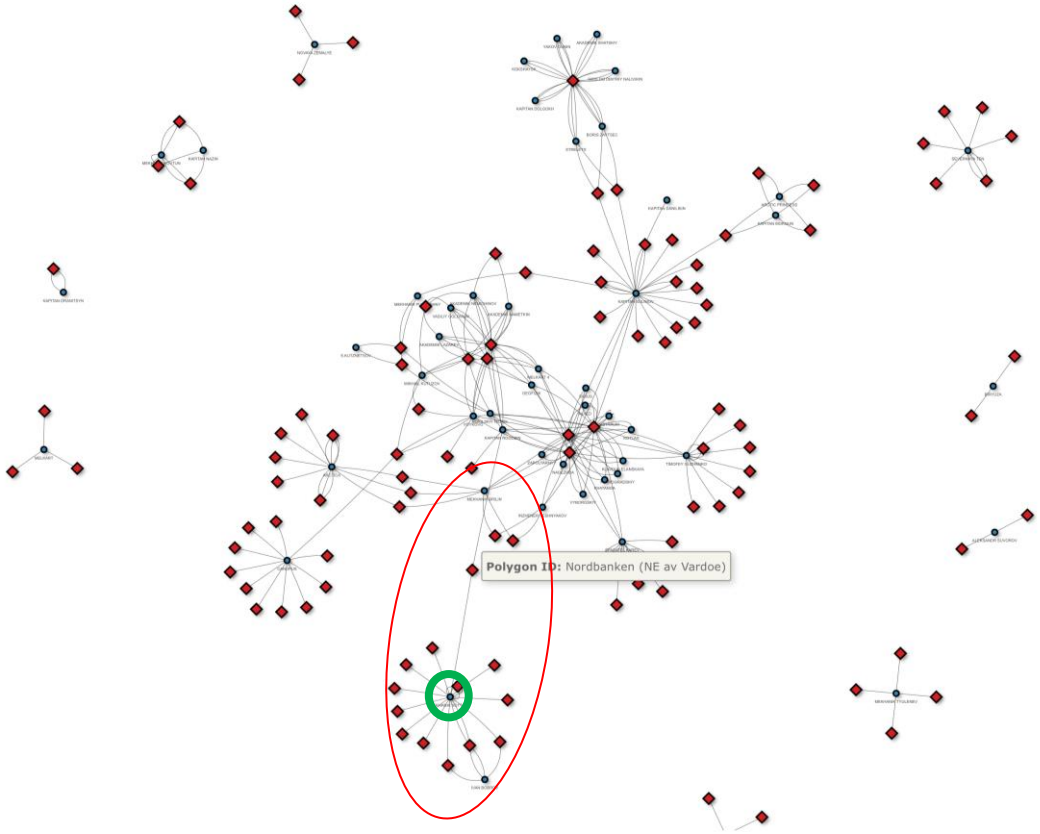
Figur 8.23 viser hvordan man ved å følge *stier* i nettverket kan finne frem til andre aktører som har tilknytning til et bestemt nettverk. I eksempelet under besøkte *«Mekhanik Pustushnyy»* og *«Sormovo 1»* Stavanger med fem dagers mellomrom.



Figur 8.23 Ved å starte med «Mekhanik Makarin» utenfor Vardø, har nettverket en *sti* (avstand) på 6 kanter til «Sormovo 1» til kai i Stavanger.

Et annet funn fra mai er den russiske yachten *«Elden»* (MMSI 273331830) og dets støtteskip *«Severnaya Ten»* (MMSI 273325210). Fartøyene seiler langs kysten og har aktivitet i området fra Kristiansand til Kristiansund frem til oktober. Aktiviteten er i stor grad tilsynelatende fokusert i farvannet mellom Ålesund og Molde. Fartøyene har i ettertid fått noe medieoppmerksomhet fordi de kyttes til den russiske ogliarken Oleg Deripaska som har tette forbindelser til Kreml og Putin (Joansen, 2018; Vogel & Rosenberg, 2018).

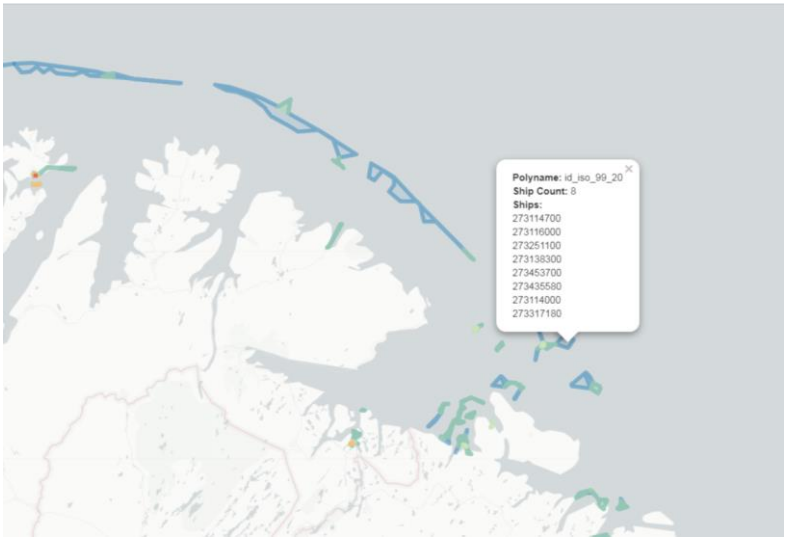
Et eksempel fra ***juni*** illustreres ved å følge *kantene «Mekhanik Kottsov»* har til andre noder i perioden. Fartøyets stopp i Stavanger, Nordsjøen, Norskehavet langs Trøndelagskysten, til kai i Mo i Rana hvor den var samlokalisert med «*Ivan Bobrov*» (MMSI 273333020), og til slutt stopp i området Nordbanken nord-øst av Vardø før den går til Murmansk, knytter en rekke andre fartøyer og områder til noden.




Figur 8.24 «Mekhanik Kottsov» (grønn sirkel) nettverk juni 2014.

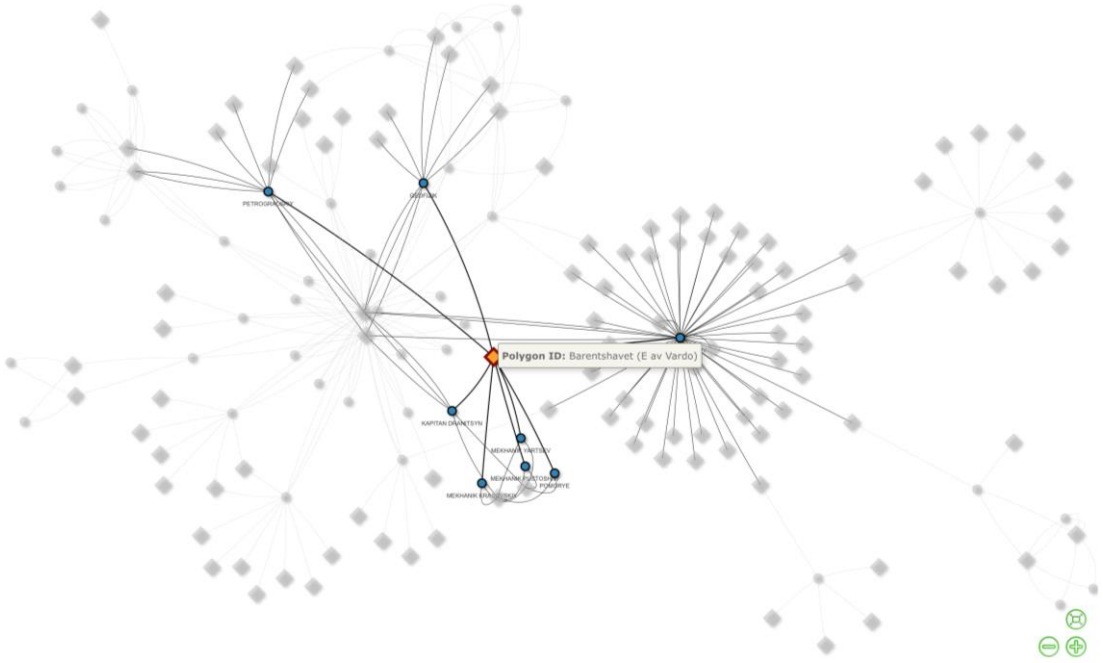
Visualisering kan bidra til økt situasjonsbevissthet rundt de omkringliggende faktorer, og se enkeltfartøyers adferd i en større sammenheng. Figur 8.24 illustrerer dette.

Figur 8.25 illustrerer et bilde av fartøyer som har operert i et definert område i ***Juli***. Dette er gjort for å illustrere muligheten til å analysere nettverksstrukturer med utgangspunkt i en geografisk posisjon. Det aktuelle området har høy grad av mellomleddssentralitet, hvor det geografiske punktet, eller noden, fungerer som en *bro* eller en såkalt *portvokter* mellom klynger i et nettverk. En klynge defineres som ulike undergrupper der nodene har relativt tette relasjoner (Everton, 2012, s. 12). Eksempler på klynger kan være fiskefartøyer som driver fiskeriaktivitet i nærheten av hverandre over tid, eller fartøyer som ligger til kai i samme havn.



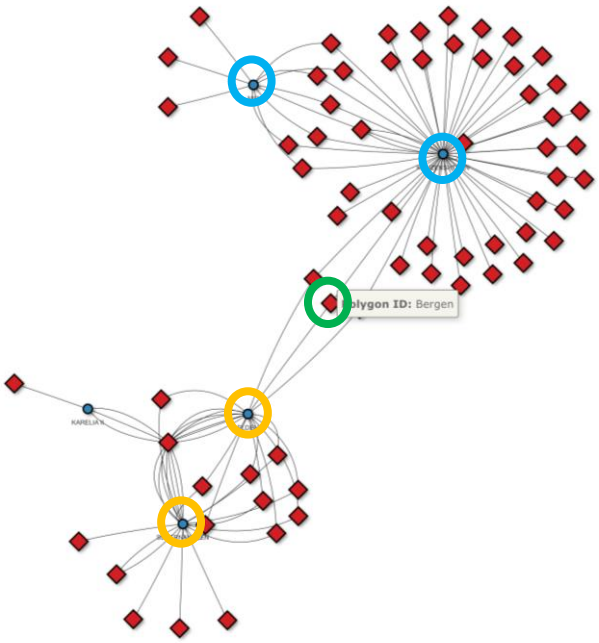

Figur 8.25 «Point of Interest» Barentshavet (E av Vardø) hvor åtte ulike fartøy eid av to kommersielle selskaper samt to russiske statseide fartøyer, «Kapitan Dranytsin» (MMSI 273138300) og «Geofizik» (MMSI 273453700) oppholdt seg.

Figur 8.26 under viser hvordan registrerte stopp i Barentshavet som vist i figur 8.24 kan fungere som et nav med høy grad av mellomleddssentralitet, og dermed viktig for å nå andre deler av nettverket. De andre punktene i nettverket under med høy grad av sentralitet er havnene Murmansk og Kirkenes. Begge havnene er sentrale «aktører» som har relasjonelle sammenknytninger med en rekke av fartøyene i studien.




Figur 8.26 Nettverksutbredelse fra «Point of Interest» Barentshavet (E av Vardø) (oransje firkant). Blå noder viser åtte fartøyer som har stoppet i punktet i løpet av juli.

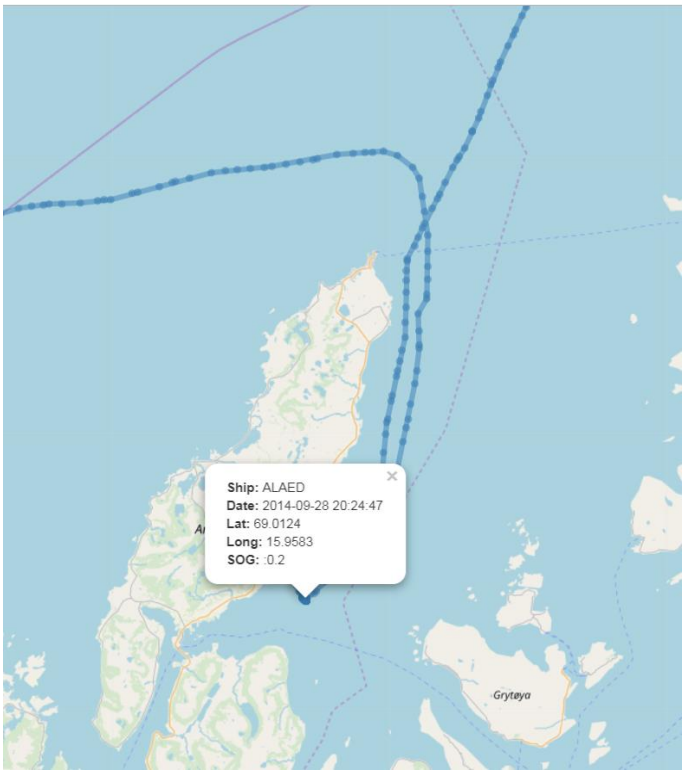
Videre registreres seilas av de to russiske statseide seilfartøyene *«Mir»* (MMSI 273133800) og *«Kruzenshtern»* (MMSI 273243700) i forbindelse med Tall Ships Race 2014. . *«Kruzenshtern»* og yachten *«Elden»* lå begge til kai i Bergen. Fartøyene lå ikke til kai samtidig. Bergen havn som eksempelet i dette nettverket illustrerer allikevel i likhet med «POI» Barentshavet en høy grad av *mellomleddssentralitet* da nettverkets cluster knyttes sammen i dette punktet.




Figur 8.27 Nettverksstruktur juli 2014: «Elden-Bergen-Kruzenshtern» fra valgt «Point of Interest» Bergen (grønn sirkel). «Elden» og «Severnaya Ten» (oransje sirkel), «Kruzenshtern» og «Mir» (blå sirkel)

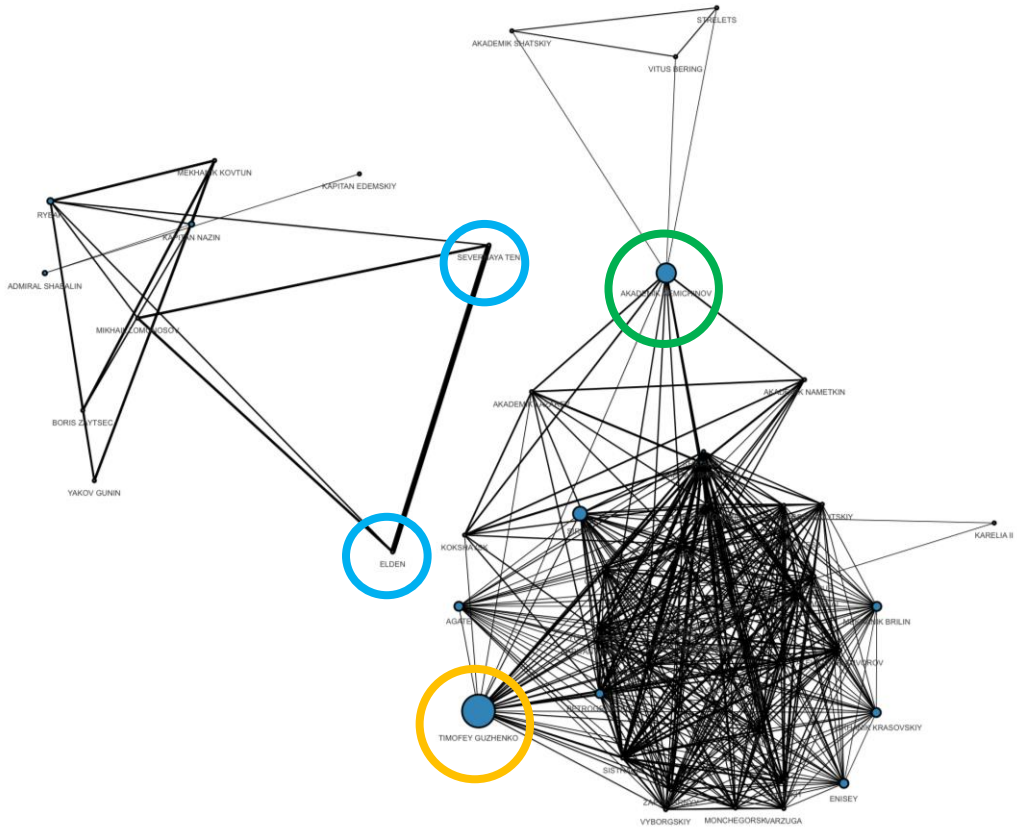
***August og september*** viser tilsvarende aktivitet som de foregående månedene i 2014. *«Elden»* og *«Severnaya Ten»* seiler i området fra Ålesund til Kristiansund i hele august, mens det i september kun foretar korte seilaser ut fra Ålesund. Fartøy av interesse som registreres for første gang, er blant annet «*SCF Pechora*» (MMSI 273340570) som tilhører selskapet *Sovcomflot (SCF)*, der Russlands nåværende assisterende transportminister, Viktor Olerskiy er styremedlem (Sovcomflot, 2018). Farley og Meskos antakelse i rapporten «The Odessa Network» er at det eksisterte stor grad av tillit mellom kontraktør og myndigheter i tilfeller der sensitive oppdrag skulle løses på vegne av den russiske stat (Wallace & Mesko, 2013, s. 9). Nevnte Olerskiy var

også tidligere styremedlem i *North-Western Shipping Company* (Wallace & Mesko, 2013, s. 46). Figur 8.28 viser *«Alaed»* (MMSI 273355170) beskrevet innledningsvis i dette kapittelet. Fartøyet gjennomførte sensitiv våpentransport til Syria i 2013. Fartøyet oppholder seg i Andfjorden fra 27. september før det setter kursen videre sydover om kvelden 28. september 2014.



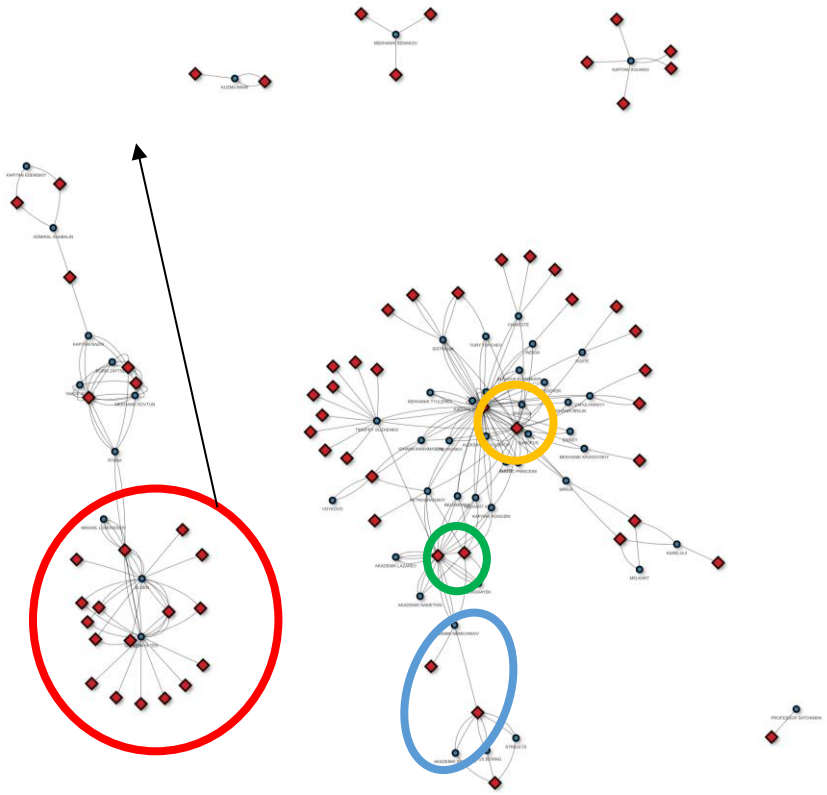

Figur 8.28 «Alaed»ved Andøya 28. september 2014

I ***oktober*** viser analysen at fartøyene med høyest grad av mellomledssentralitet (betweeness) begge er russiske statseide fartøyer. Disse er henholdsvis *«Timofey Guzhenko»* (MMSI 273330620) og *«Akademik Nemchinov»* (MMSI 273454600). Gradssentralitet forteller oss hvor mange kanter en node har knyttet til seg. Høy mellomleddsentralitet karakteriserer noden i nettverket som ligger langs den korteste «stien» som forbinder alle andre par med noder i nettverket. Figur 8.29 viser nettverket basert på fartøyers samlokalisering for oktober der størrelsen på nodene representerer mellomleddssentralitet (betweeness). Noder som ikke er knyttet sammen med det øvrige nettverket representerer noder som ikke har noen registrert samlokalisering med andre noder i nettverket. Blant disse finner vi den russiske yachten *«Elden»* og støttefartøyet *«Severnaya Ten»* som blant annet besøkte Ålesund, Austevoll syd for Bergen, og Stavanger denne høsten.




Figur 8.29 Mellomleddsentralitet oktober. Grønn sirkel markerer «Akademik Nemchinov», oransje sirkel markerer «Timofey Guzhenko». Blå sirkler indikerer «Elden» og «Severnaya Ten». Tykkelsen på kanten mellom sistnevnte indikerer høy grad av samlokalisering. De har opptrådt sammen i de samme geografiske punktene.

Utstrekningen av russiske maritime nettverk i norske interesseområder er stor, og normalsituasjonen er kontinuerlig russisk tilstedeværelse i hele interesseområdet vårt. Figur 8.30 illustrerer dette.

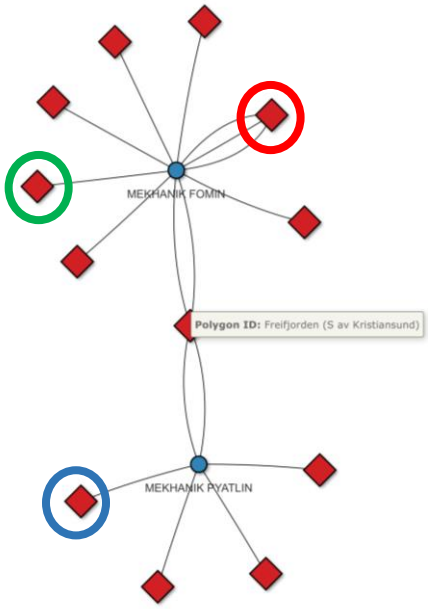


Figur 8.30 Nettverkets utstrekning. Markert med rød sirkel Oleg Deripaskas *«Elden»* og *«Severnaya Ten»* seilas fra Ålesund til Kristiansand. Røde firkanter markerer stopp. Nettverkets utstrekning i pilens retning strekker seg til Færøyene. Blå sirkel markerer aktivitet knyttet til Olavsvern, grønn Kirkenes og gul Murmansk.

Ved å ta et tilbakeblikk på figur 2.1 innledningsvis i denne oppgaven viser Diesen til hvor utfordrende det vil være å se hvordan hendelser passet inn i et større mønster, og at slike påstander i samtid vil kunne fremstå eller fremstilles som utslag av paranoid holdning (Diesen, 2018, s. 22). Skulle man i en gitt situasjon ønske å benytte denne muligheten til teste norsk evne til å se sammenhenger eller å skjule en hybrid trussel ser man hvor utfordrende det vil være å oppdage et slikt avvik.

Analysen av perioden ***november til desember*** viser en konsentrasjon av nettverksaktivitet i Barentshavet øst og nord-øst av Vardø samt en del trafikk rundt Andøya. Studien gir også en bekreftelse av russiske seismikkfartøyers bruk av den nedlagte marinebasen på Olavsvern. *«Akademik Nemichinov»* (MMSI 273454600) og *«Akademik*

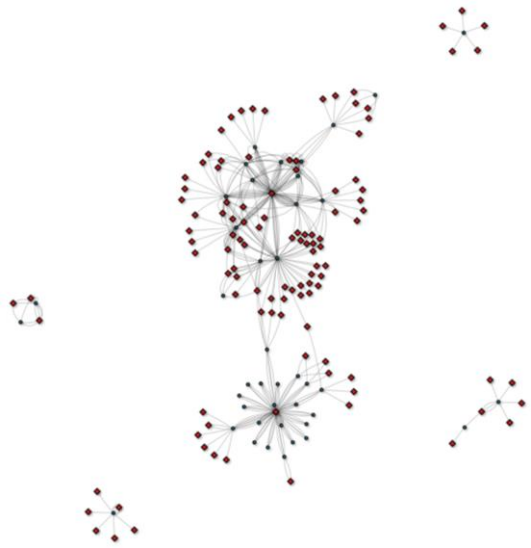
*Shatskiy»* (MMSI 273452600) benyttet seg i perioden henholdsvis av Olavsvern og Tromsø havn. Figur 8.31 oppsummerer hvordan den maritime nettverksanalysen for 2014 har bidratt til å få frem mønster og sammenhenger. Eksempelet er fra desember måned og tar utgangspunkt i Freifjorden syd av Ålesund. To fartøy har vært samlokalisert her, og når man ekspanderer dette nettverket vil andre noder synliggjøres. Grønn ring markerer Fensfjorden nord for Bergen. Rød ring markerer Lødingen. Blå ring markerer Vesterålen.



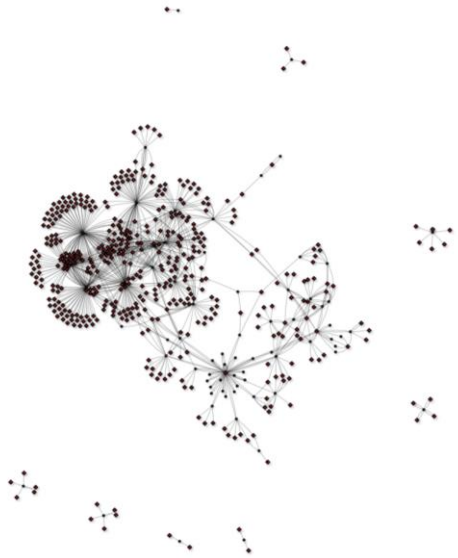

Figur 8.31 Maritim nettverksanalyse desember med utgangspunkt i Freifjorden (syd av Kristiansund)

# 8.2 Maritim nettverksanalyse 2017

Størrelsen på datasettet for 2017 inneholder en signifikant større mengde data grunnet flere registreringer pr fartøy sammenlignet med 2014. Dette henger sammen med at vi i dag har satellittdekning av fire satellitter, mens det i 2014 var kun èn satellitt (AISSat-1) før AISSat-2 ble skutt opp juli 2014 (Kystverket, 2017a). Dette påvirker antall registreringer, og dekningsområdet for satellittene er større. Dette gir høyere oppløselighet på målingene, og registrerer fartøy i større geografisk utstrekning enn i 2014. Figur 8.32 og 8.33 illustrerer dette. 2017 analysen har resultert i en utvidelse av totalt antall fartøyer til 156. Antall selskaper eller eiere er økt til 49.



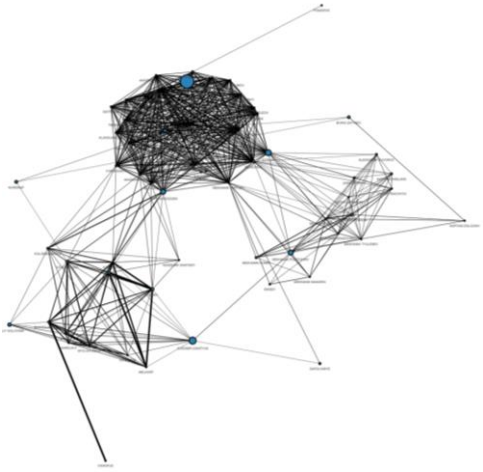
Figur 8.32 Fartøy-stopp punkt januar 2014



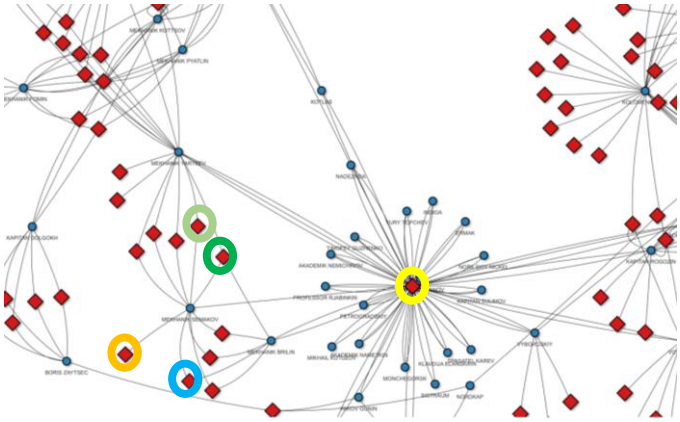
Figur 8.33 Fartøy-stopp punkt januar 2017

Ser vi på **januar**, og tar noden som i nettverket ligger langs den korteste «stien» som forbinder alle andre par med noder i nettverket finner vi *«Mekhanik Semakov»* (MMSI 273113800). Figur 8.35 til høyre under viser hvordan noden knytter det maritime nettverket sammen ved blant annet å ha stoppet i Murmansk (gul), Onega (grønn), Sarnesfjorden like

vest av Honningsvåg (blå), Vestfjorden (oransje), Vannvågen syd av vannøya i Troms (lys grønn).

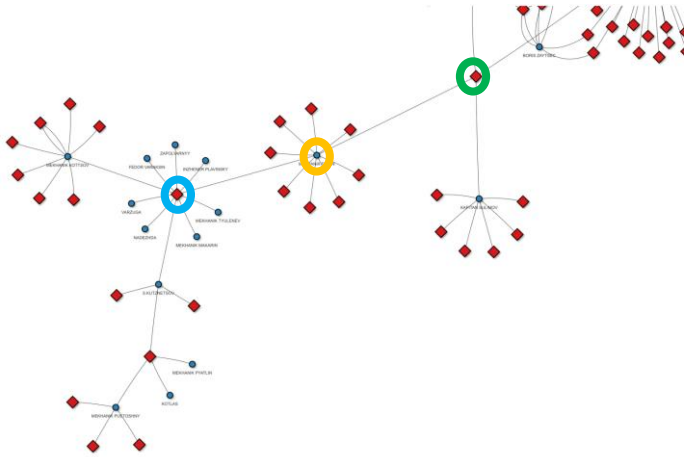


Figur 8.34 «Mekhanik Semakov» blå node



Figur 8.35 «Mekhanik Semakov» januar 2017

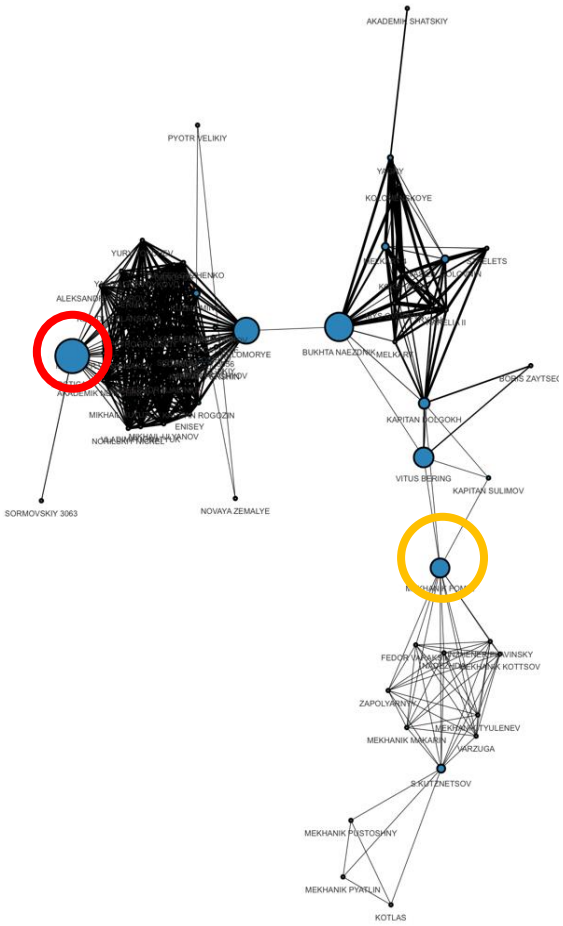
To multinasjonale øvelser ble avholdt i bergensområdet fra 6. – 17. **februar**. «Standing NATO Maritime Group-1» (SNMG-1) deltok på begge øvelsene og sikret slik en samlet deltakelse på 12 fartøy fra ulike nasjoner (NATO, 2017a). En av nodene som scorer høyt på sentralitet er «*Mekhanik Fomin*» som ved stopp både i Ålesund og Arkhangelsk kan sees på som en «broker» i mellom flere *klynger* i ulike nettverk.



Figur 8.36 «Mekhanik Fomin» (oransje sirkel) som sentral node mellom nettverk med utspring i Arkhangelsk (blå) og Ålesund (grønn)

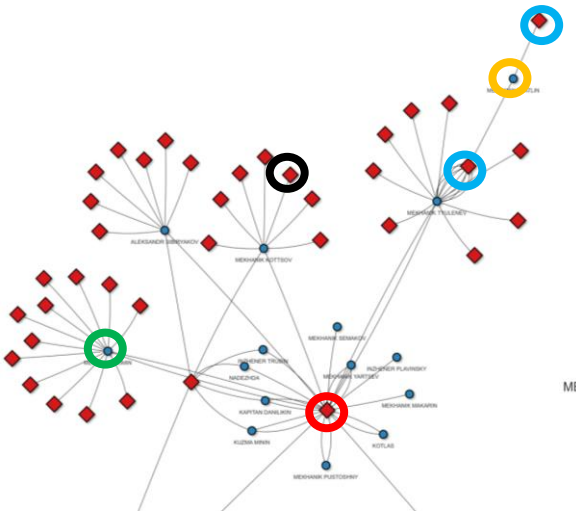
Også lastefartøyet «*Arctica 1*» (MMSI 273386130) som dukker opp for første gang i analysen, har både høy grads og mellomledd-sentralitet. Antallet kanter til andre fartøyer er 24. Noden skaper således en relasjon mellom Murmansk havn og fartøyet «*Sormovskiy 3063*»

som er eid av *Northern-Shipping Company*. Begge hadde gjentatte stopp i bergensområdet denne måneden.

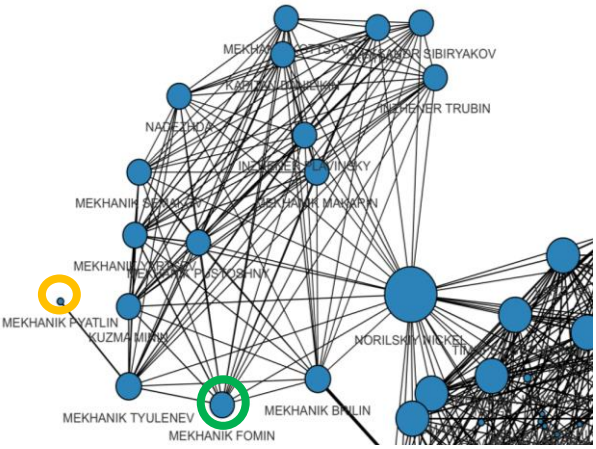



Figur 8.37 «Arctica 1» (rød sirkel). «Mekhanik Fomin» (oransje sirkel)

Øvelse «Joint Viking» ble gjennomført i Finnmark 6. -15. **mars** i området fra Alta til Lakselv. Aktiviteten foregikk hovedsakelig langs kysten (Forsvaret, 2017). Flere av nodene knyttet til avvik i mars 2014 finner man også igjen i analysen av 2017. *«Mekhanik Pyatlin»* og *«Mekhanik Fomin»* er to av flere fartøyer med registrerte avvik samme måned begge år. Områdene dette forekommer i er riktignok ikke de samme. Dette kan allikevel indikere et mønster. I figurene under er de markert med henholdvis oransje og grønn sirkel. Grå sirkler markerer stopp i ulike deler av Nordsjøen. Sort sirkel markerer stopp nord av Andøya. Rød sirkel markerer Arkhangelsk.

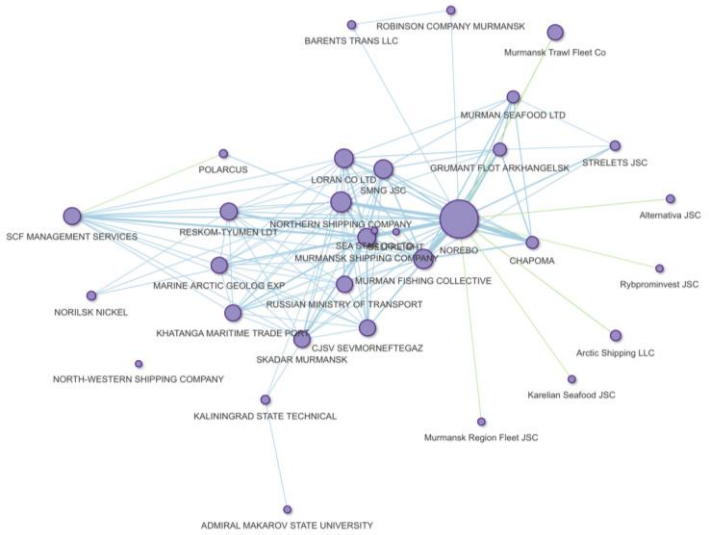


Figur 8.38 Mars 2017 Fartøy (blå noder)-Stopp (røde noder)



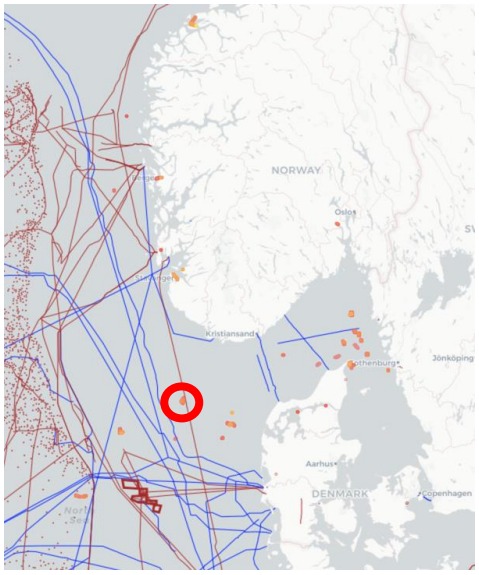

Figur 8.39 Størrelse på blå noder indikerer gradssentralitet

Analysen for **april og mai** viser ingen store endringer i nettverkenes aktivitet. Figur 8.40 viser et representativt bilde selskapsstruktur basert på fartøyers samlokalisering.

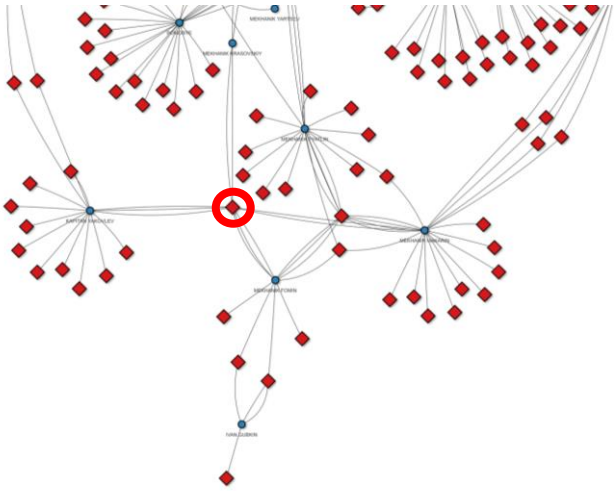



Figur 8.40 Nettverket av eierstrukturer og gradssentralitet, som bestemmer størrelse på noder. Nettverket baseres på fartøyenes samlokalisering i mai 2017. Fiskerikonglomeratet Norebo har en gradssentralitet på 39 mens Northern Shipping Company har en gradssentralitet på 17.

Et eksempel fra **juni** bidrar til å illustrere hvordan stordata og SNA kan bidra til bedre situasjonsbevissthet rundt kritisk infrastruktur. Figur 8.41 viser fire ulike fartøyer som alle har stoppet i det samme området i nærheten av oljerørledningen Europipe II som leverer gass fra Kårstø i Rogaland til Dornum i Tyskland. Alle de fire fartøyene tilhører NSC.

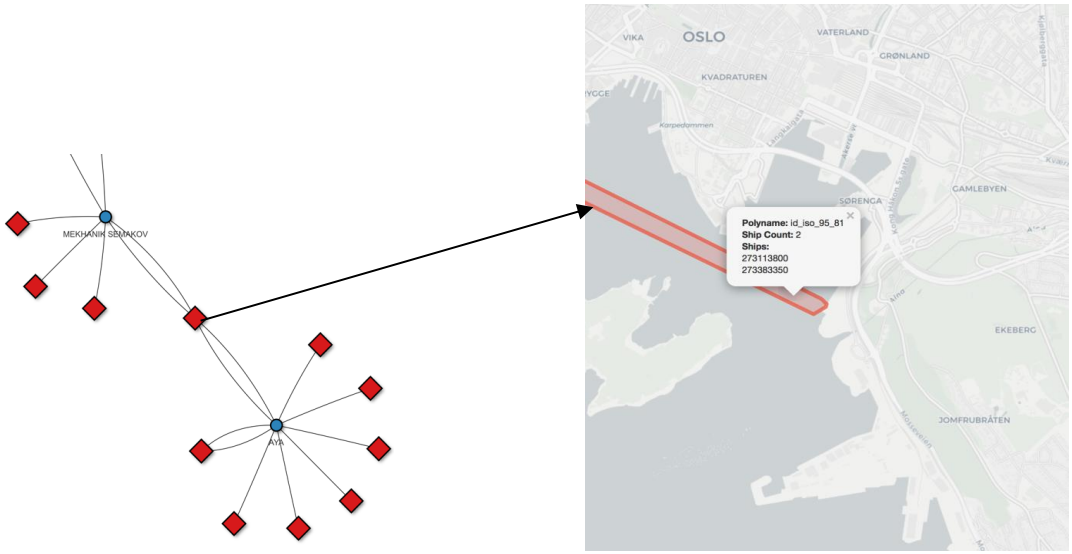



Figur 8.41 Samlokalisering fire fartøyer Europipe II



Figur 8.42 Polygon for samlokalisering markert med rød sirkel.

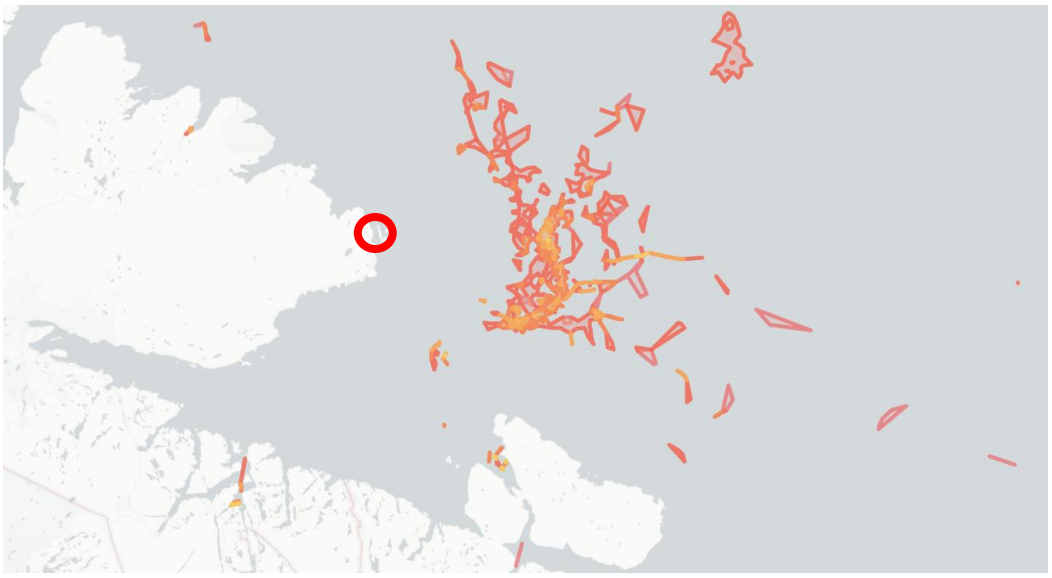
Man kan også finne fritidsfartøyer på mindre enn 300 tonn som bruker AIS. Eksempelet under viser dette, og visualiserer stoppunkter for seilfartøyet «*Aya*» (MMSI 273383350) sin ferd langs kysten i **juli.** Når man analyserer potensielle grå maritime nettverk, kan man som tidligere illustrert med yachten *«Elden»*, ikke utelukke sivile ikke kommersielle friditsfartøyer. Videre som figur 8.43 viser var også *«Mekhanik Semakov»* i Oslo i juli 2017.



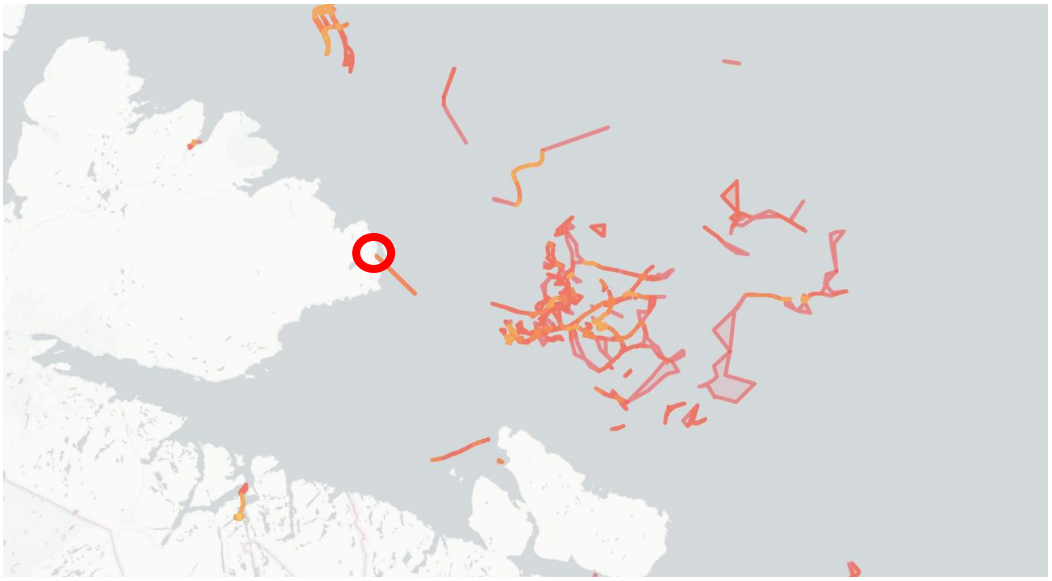

Figur 8.43 Nettverk med utgangspunkt i seilbåten «Aya» og pil markerer polygon i kartet hvor samlokalisering er registrert.

**August** representerer et funn som bekrefter en trend som viser økende aktivitet fra maritime nettverk i områdene øst av Finnmark og POI Vardø i 2017 sammenlignet med 2014. Fartøyene består for det meste av fiskefartøyer som bedriver fiske på Nordbanken,

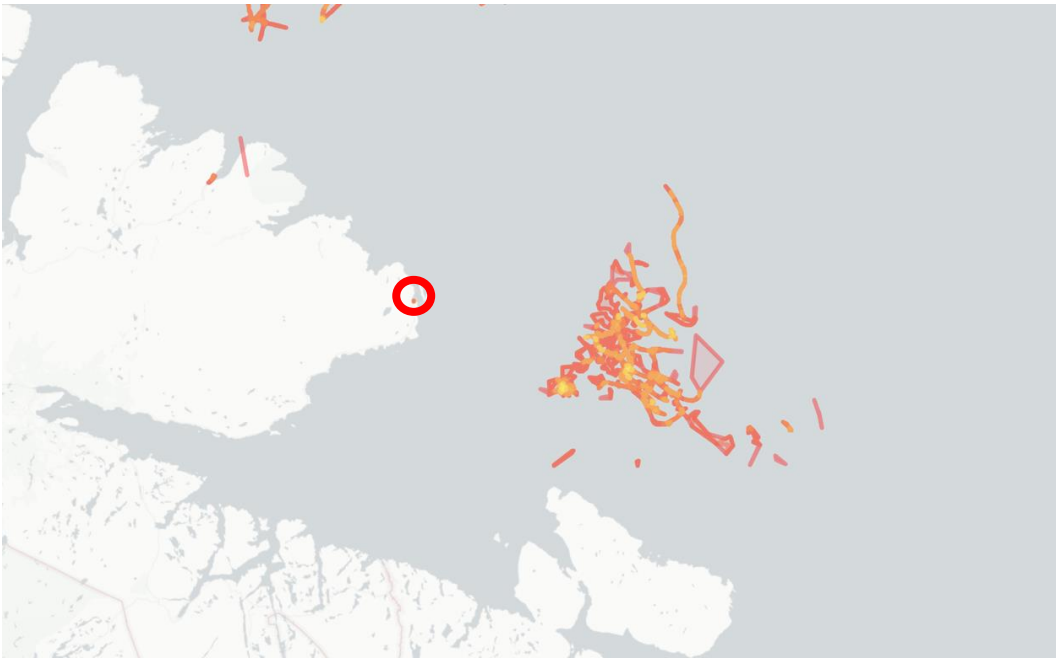
Skolpenbanken eller Østbanken. Fremstillingen i figurene under er tatt med for å illustrere en «normalsituasjon» i perioden fra mai og frem til august 2017. Registrerte avvik i form av stopp er allikevel knyttet til enkeltfartøyer som i alle er eid av *Northern Shipping Company*. I snitt har 4,5 fartøyer knyttet til dette selskaper stanset over tid i et eller flere områder i disse fiskefeltene. Ingen andre avvik tilknyttet ordinære transportselskaper er registrert.



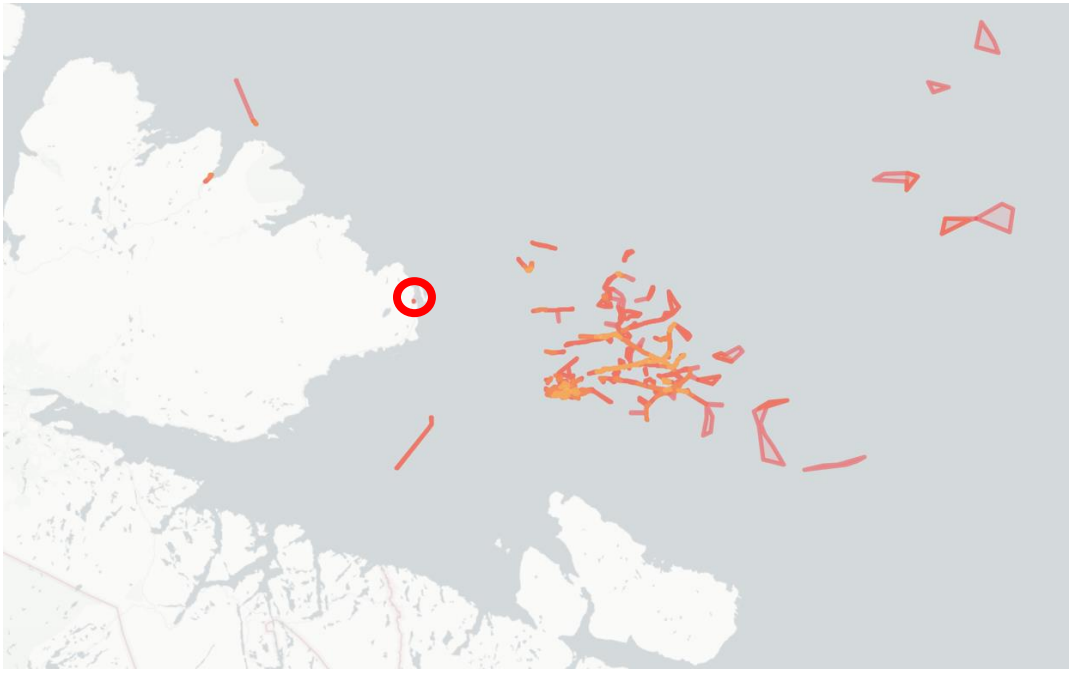
Figur 8.44 Barentshavet Vardø POI mai 2017



Figur 8.45 Barentshavet Vardø POI juni 2017



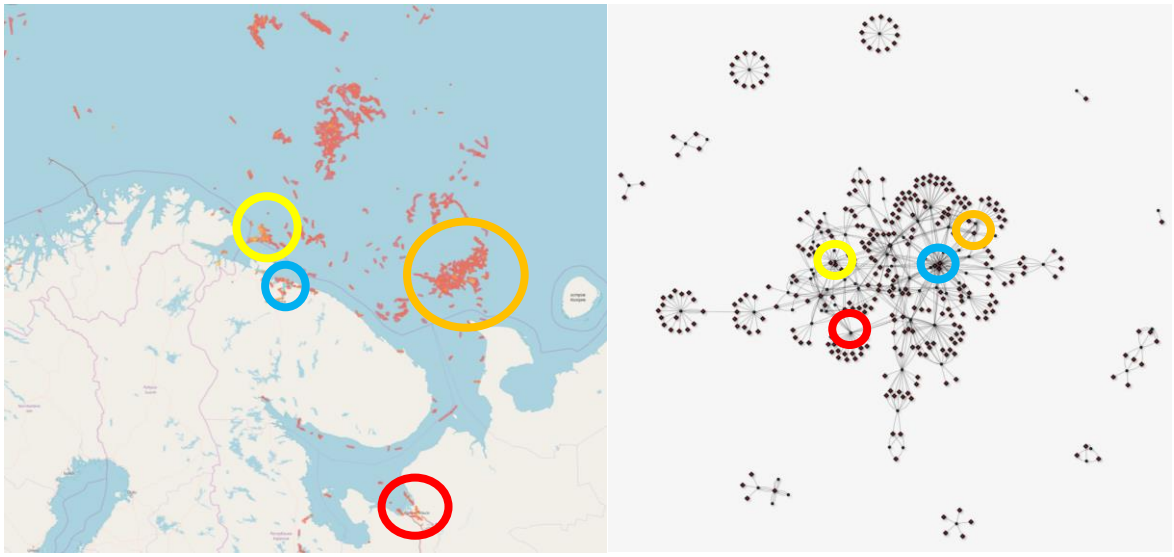
Figur 8.46 Barentshavet Vardø POI juli 2017



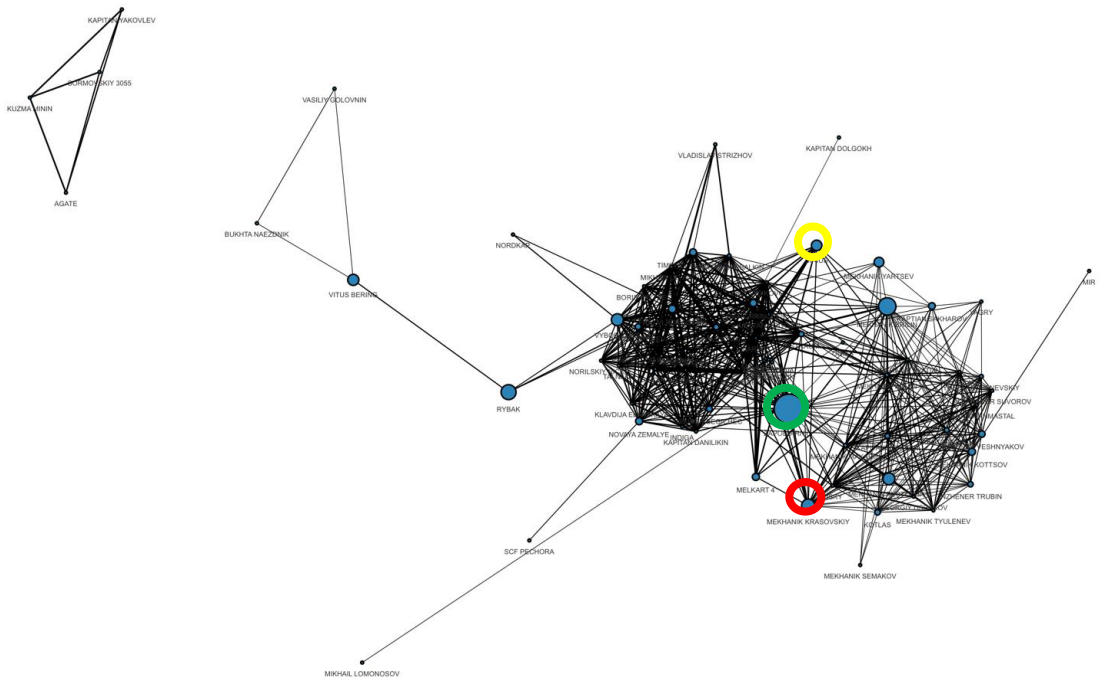
Figur 8.47 Barentshavet Vardø POI august 2017

Øvelsen *Zapad 2017* ble gjennomført (på NATOS østflanke) i det vestlige russiske militærdistrikt fra 14.-20. ***september 2017***. Øvelsen hadde en strategisk karakter hvor storskala mellomstatlig konflikt ble øvd. Aktiviteten i nordflåtens (arktiske) militærdistrikt ble registrert som særlig intens (NATO, 2017b). Figur 8.48 under viser aktivitet knyttet til

havnene Murmansk og Arkhangelsk samt tilhørende maritime nettverk som opererer i henholdsvis havområdet øst av Vardø samt havområdet nord av Kolahalvøya. Fargekodene gjenspeiler de fire utvalgte områder med samme farge.



Figur 8.48 Russiske maritime nettverk september 2017.

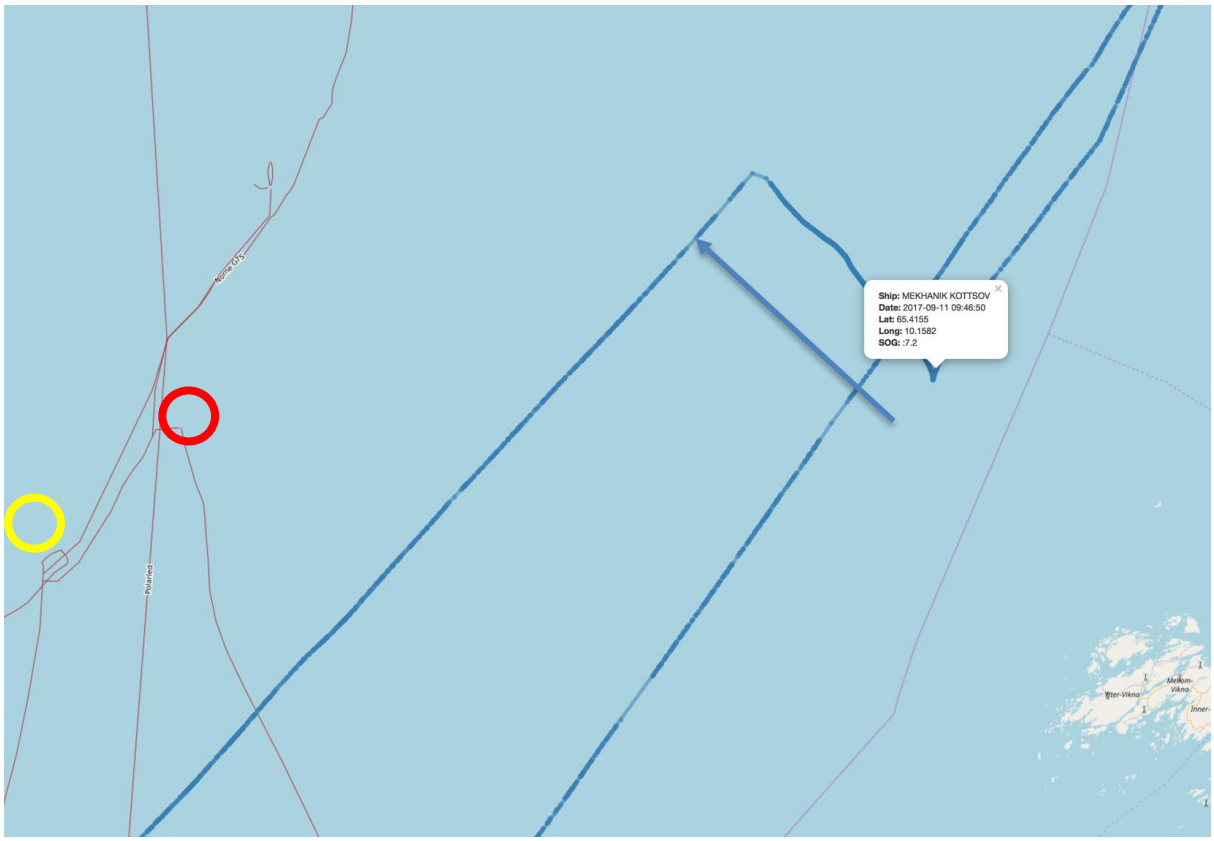



Figur 8.49 Mellomleddssentralitet september 2017. «Zapolarnyy» marert i grønn, «Mekhanik Krasovskiy» markert i rødt. «Mekhanik Brilin» markert i gult.

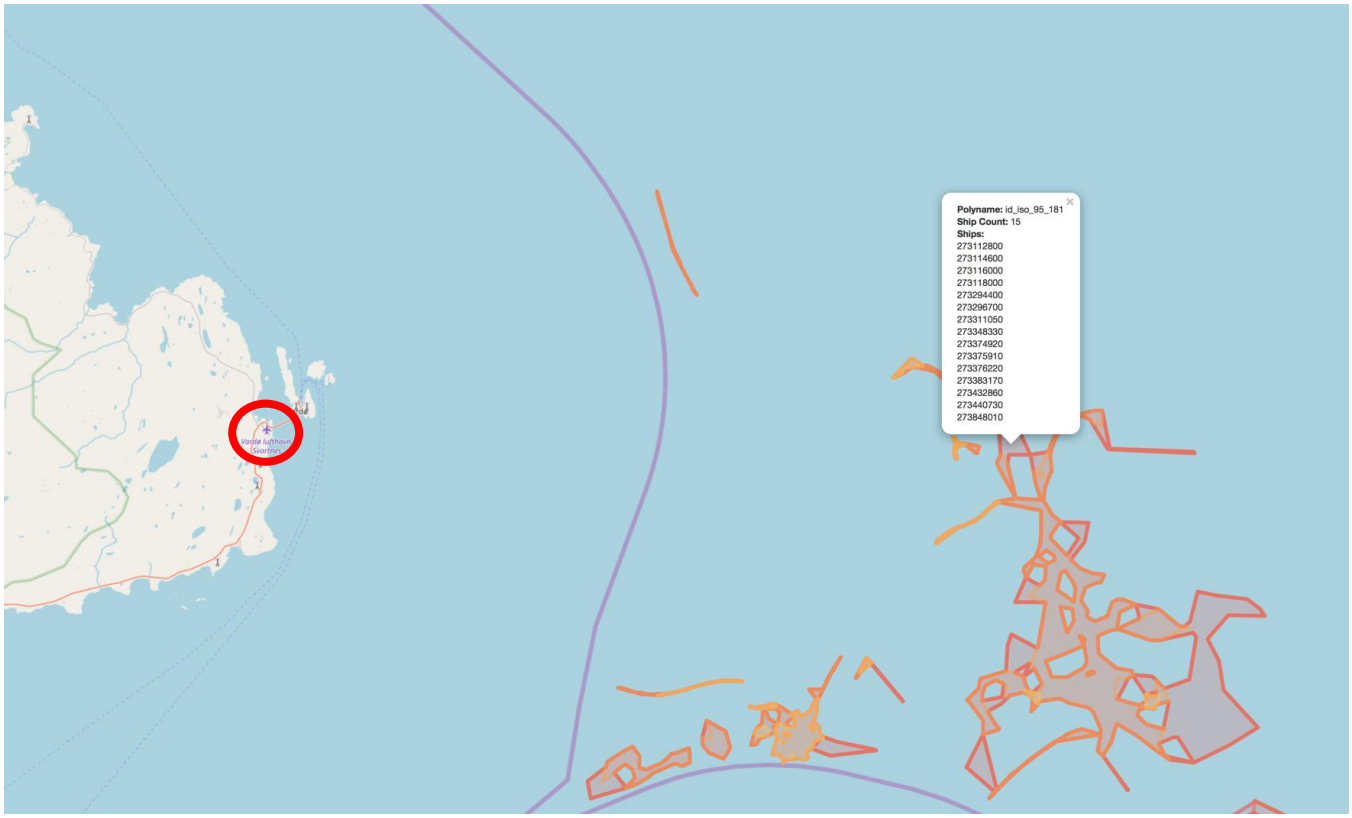
Figur 8.49 viser noder sortert på nettverkets mellomleddssentralitet for september. «*Zapolarnyy*» (MMSI 273349820) er fartøyet med høyest grad av mellomleddssentralitet. Fartøyet oppholder seg i september både i Murmansk og i Arkhangelsk.

«*Mekhanik Krasovskiy*» er et annet fartøy som skiller seg ut med avvikende adferd med stopp syd i Nordsjøen, Nordsjøen utenfor Stavanger, og i havområdet øst av Vardø. «*Mekhanik Brilin*» har også høy grad av mellomleddsentralitet og er en sentral node blant mange fartøyer som i september gjennomfører stopp i områdene øst av Vardø. «*Mekhanik Fomin*», «*Mekhanik Pyatlin*» og «*Belomorye*» er eksempler på slike. Samtidig pågår det fiskeriaktivitet i området. Det er også avvik i nærhet av kommunikasjonskabler og olje og gassinfrastruktur i Nordsjøen og i Norskehavet. Tankfartøyet «*Anchinov Bridge*» eid av *SCF* stopper like ved kommunikasjonskabelen Atalantic Crossing 1 (AC1).

«*Mekhanik Kottsov*» går med sakte fart under 1,5 knop fra 11. september kl 0945 og øker farten igjen 12. september kl 0706. Manøveren vises på figuren under. Fartøyet gikk på en nordvestlig kurs i 22 timer og tilbakela en distanse på 26 nautiske mil (49km) som indikerer en snittfart på mellom 1,1 og 1,2 knop.



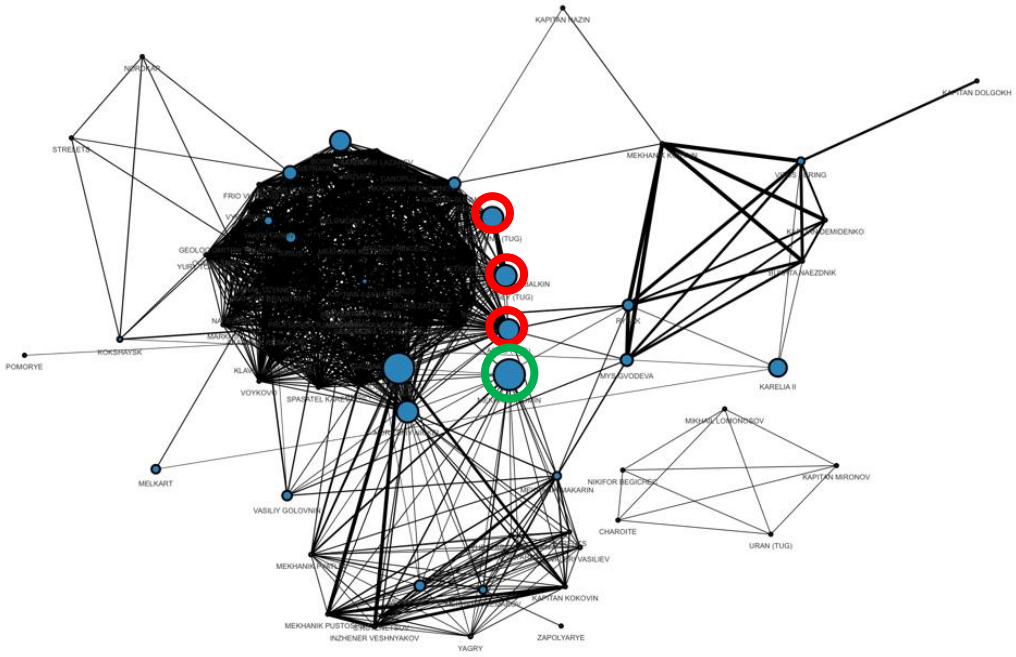

Figur 8.50 «Mekhanik Kottsov» 11.- 12. september 2017. Pilens lengde tilsvarer 26 nautiske mil. Gul sirkel markerer geografisk posisjon av «Åsgård feltet». Rød sirkel markerer geografisk posisjon «Heidrun feltet».



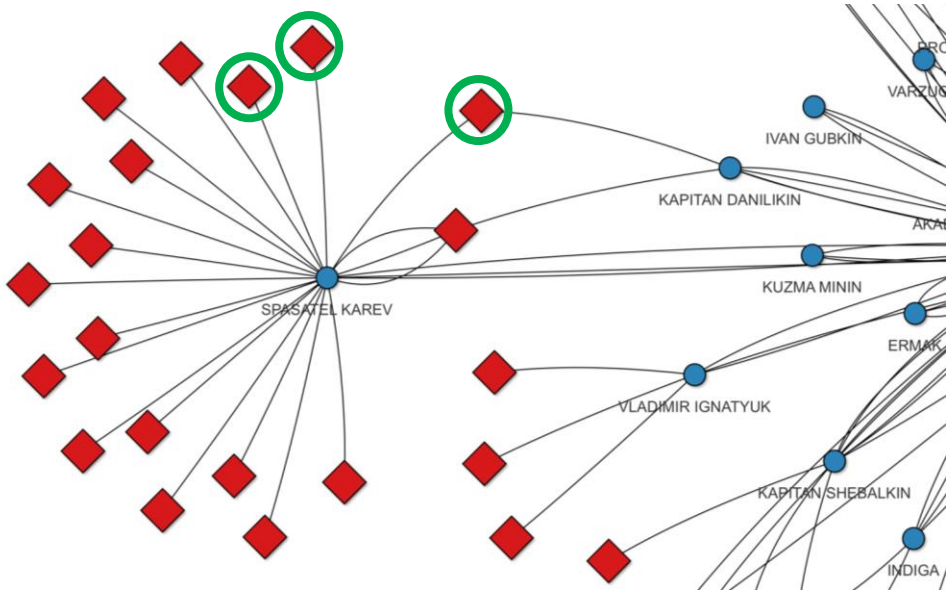

Figur 8.51 «POI Vardø» (rød sirkel) og aktivitet på Østbanken

Følger man antall *kanter* i septembernettverket viser analysen blant annet at antall kanter, geodetisk avstand, fra Ytre Oslofjord til området vest av Vardø er fire.

Aktiviteten rundt Vardø reduseres i perioden fra ***oktober*** til ***desember*** og analysen viser at nettverkene samlokaliseres andre steder. Analysen viser at et økende antall russiske slepebåter opererer i nettverksstrukturen årets siste tre måneder. Dette er ikke observert i like stor grad tidligere i oppgaven. Eksempel på dette er slepebåten «*Argo*» (MMSI 273399790) som blant annet gjennomfører stopp i Korsfjorden sør for Bergen og i Ålesund. Øvelsen «FLOTEX 2017» ble gjennomført i perioden 13. – 1. desember 2017 i området fra Bergen til Troms fylke. Slepebåtene «*Nordsund*» (MSSI 273350540) og «*Odissey*» (MMSI 273380520) gjennomfører i november stopp i Saltfjorden like syd for det sentrale øvelsesområdet i Vestfjorden. «*Mekhanik Fomin*» er et av fartøyene som med høy grad av mellomsentralitet som også opptrer i nær forbindelse med samtlige andre nettverk i analysen for november.




Figur 8.52 Noder sortert etter mellomleddsentralitet november 2017. Jo større sentralitet jo større noder. Slepebåtene «Argo», «Norsund» og «Odissey» markert med rød ring. «Mekhanik Fomin» markert med grønn ring.




Figur 8.53 «POI» Andøya desember 2017. Grønne sirkler markerer stopposisjoner vest og nordvest av Andøya.

Figur 8.53 viser at det statseide russiske fartøyet *«Spasatel Karev»* og *«Kapitan Danlikin»* eid av *Murmansk Shipping Company* stopper i samme posisjon utenfor Andøya i desember.

## 8.3 Hva forteller resultatene oss?

Analysen gir følgende resultat. Ved å benytte en kombinasjon av stordata og sosial nettverksanalyse har analysen kartlagt et totalt antall på 156 fartøyer fordelt på en eierstruktur bestående av 49 private og stalige russiske selskaper. Et stort antall stoppunkter i norske interesseområder er også registrert gjennom de to år oppgaven tar for seg. De fleste av nettverkene i denne oppgaven driver næringsvirksomhet der russiske selskaper samarbeider med norske næringsinteresser. Samtidig viser funnene i oppgaven at enkelte av aktørene i tillegg kan ha andre interesser enn kun de merkantile. Utfordingen med nettverkenes adferd er at det er vanskelig å skille slike avvik fra uskyldige hendelser. Den maritime nettverksanalysen peker på koblinger mellom det russiske statsapparatet og aktørene som er avdekket. Oppgaven indikerer mer enn en gang en direkte tilknytning til blant annet *Odessanettverket*, eller andre russiske statlige aktører og interesser. Gjennom bruk av stordata og sosial nettverksanalyse viser analysen indikasjoner på sammenhenger og mønster.

Til tross for oppgavens vektlegging av og avgrensning til russisk helhetlig tilnærming og russisk maritim doktrine er det viktig med balansegang i forhold til hvordan resultatene tolkes. Som nevnt tidligere i oppgaven er det en rekke tilfeller der slik adferd kan forklares med at dette er uskyldige hendelser. I denne forbindelse er det viktig å gjenta at oppgavens ambisjon ikke har vært å gjennomføre en fullstendig analyse av samtlige potensielt mørke eller grå russiske nettverk i norske interesseområder, men som et «proof of concept». Samtidig kan man ikke se bort fra at avvik, som at russiske sivile fartøyer driver etterretningsvirksomhet i norske interesseområder, er representert i funnene. Avvikene som oppgaven refererer til er sågar basert på et avgrenset filter påvirket av blant annet behovet for å forenkle stordatasettet, og tilpasse dette tilgjengelig dataprosesseringskapasitet i forbindelse med studien. Videre er kategorier av adferd i denne oppgaven i mange av tilfellene et resultat av en «normaltilstand» hvor denne av naturlige årsaker kan tilskrives for eksempel embarkering av los, at fartøyer ligger værfast, gjennomfører maskinøvelser og så videre.

Bruk av stordata og SNA gir til tross for dette muligheter til å avdekke mønster og endringer i nettverk over tid. Implementert i eksisterende systemer for maritim situasjonsbevissthet, vil dette kunne gi viktig tilleggsinformasjon. Utfordringen vil alltid være å skille adferden fra maritime hybride trusler fra det som er normalsituasjonen. Selv med bruk av stordata og SNA vil det altså være utfordrende å identifisere avvik. På en annen side tilfører metodene fra SNA muligheter til å triangulere funn med andre nettverksstrukturer. Potensiale i å også benytte andre tilgjengelige ugraderte og graderte kilder inn i SNA av AIS-

data vil bidra til en økt innsikt og mulighet til å registrere avvik. Analyse av sosiale medier som en node i nettverkstrukturen er ett eksempel på dette. Dette er viktig å huske på når resultatene i denne oppgaven vurderes.

## Nettverkstrukturer

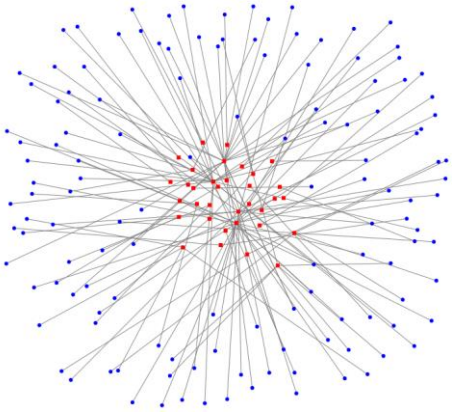
For hver måned for både 2014 og 2017 har analysen bidratt til å kartlegge nettverk bestående av fartøy, selskaper og stoppunkter. Fartøysnettverkene er satt sammen basert på i hvilken grad disse har vært samlokalisert i den aktuelle perioden. Analysen har gitt beregninger av grads- og mellomleddssentralitet for både fartøyer og selskaper. Strukturene av stoppunkter er blitt kartlagt ved å se hvor de enkelte fartøy stopper opp. Resultatene viser at de maritime nettverkene danner klynger eller «clusters» der man kan identifisere tett sammenknyttede undergrupper i nettverket. Eksempler er fiskeflåtens samlokalisering i fiskefeltene, eller fartøyers samlokalisering i ulike havner.

Selskapsstrukturer har også blitt avdekket i den maritime nettverksstrukturen. Ved å knytte fartøy, geografiske områder og selskaper sammen i to-mode nettverk har det i analysen vært mulig å også bestemme sentralitetsgrader for selskaper basert på adferden til de fartøyer de har i sin eierstruktur. *Northern Shipping Company* og *Murmansk Shipping Company* er to av de mest sentrale aktørene uavhengig av år. De eier til sammen 45 fartøyer, hvorav mange av disse har blitt registrert med avvikende adferd.

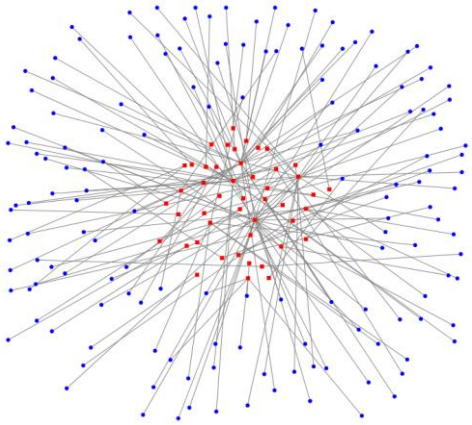
Analysen har også vist klynger rundt særskilte områder av interesse, og at sentrale aktører i de maritime nettverkene stadig opptrer rundt disse og dermed danner et mønster.

## Nettverkstetthet

Tettheten i nettverkene er et strukturelt element av sosiale og maritime nettverk. Tettheten beregnes ut ifra antallet direkte forbindelser mellom individuelle medlemmer, delt på antallet mulige direkte forbindelser i et nettverk (Kadushin, 2012, s. 29). Over tid vil man ved bruk av stordata og SNA for kartlegging av maritime nettverk i våre interesseområder, kunne bygge et godt bilde av hvordan nettverkene er knyttet sammen. Jo større nettverket er, jo mindre tetthet vil det ha fordi antall mulige kanter øker eksponensielt med hver node man legger til nettverket (Cunningham et al., 2016, s. 326).



Figur 8.54 2014 tetthet i nettverk. Eier (Rød) – Fartøy (Blå)

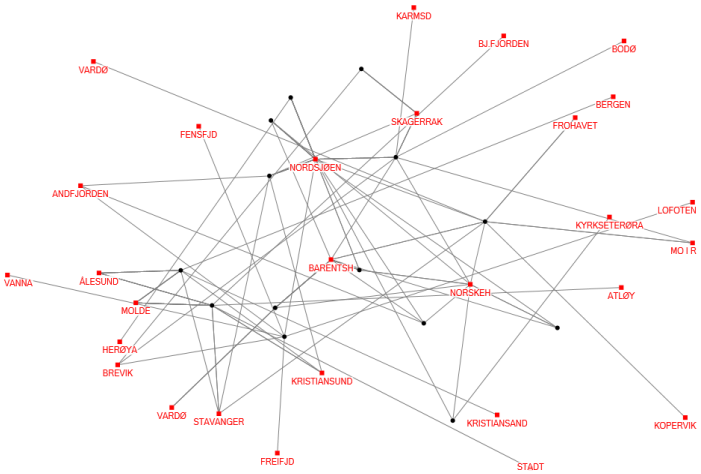


Figur 8.55 2017 tetthet i nettverk. Eier (Rød) – Fartøy (Blå)

Figur 8.54 og 8.55 illustrerer fartøy-eier struktur analysen for 2014 og 2017. Tettheten i nettverket for 2014 er 0,009, mens det for 2017 er 0,008. Dette betyr at relativt få deltakere i nettverket har en overordnet relasjon til hverandre. Nettverkene vil som eksempler fra analysen har vist, opptre med ulik grad av tetthet avhengig av hvilke noder og hvilke områder man studerer. Der alle nodene er knyttet sammen mellom alle mulige bånd vil man ha tetthet 1 i nettverket (Everton, 2012, s. 146).

## Stier

Oppgaven har ved bruk av eksempler i analysen fremhevet at den geodetiske avstanden, eller den korteste stien mellom to noder i et nettverk, kan illustrere hvordan maritime nettverk potensielt «knytter» sammen viktige deler av våre interesseområder (Cunningham et al., 2016, s. 12).




Figur 8.56 «Kategori 4» fartøyer (sort). Stoppunkter i norske interesseområder (rødt). Gjennomsnittlig geodetisk avstand er 3,33.

Som eksempel ble 12 fartøyer i 2014 vektet til kategori 4 ved at de to eller flere ganger gjennomførte flere stopp innenfor to eller flere definerte områder. Gjennomsnittlig geodetisk avstand mellom de ulike områdene er 3,33 for dette nettverket. Dette betyr at hver node i snitt må gjennom en sti på 3,33 kanter for å nå alle andre noder i nettverket.

## Sentralitet.

Sentralitet kan konseptualiseres på ulike måter. En sentral aktør kan for eksempel ha en rekke bånd til andre aktører (gradssentralitet), ha kort vei (kort stiavstand) til andre aktører, eller et mål på at en node ligger langs den korteste stien mellom en rekke andre aktører i et nettverk (mellomleddssentralitet). Disse målene kan være et uttrykk for en nodes aktivitet, og derav et mål på grad av innflytelse eller hvor viktig en node er i nettverket. Gjennom analysen er det avdekket ulik grad av sentralitet for ulike måneder og i ulike områder, og det er korrelasjon mellom funn i 2014 og 2017.

For å se hvordan et nettverk endrer seg over tid, ser man på gradssentraliteten til nettverket. Gradssentralitet bestemmes av antall relasjoner til andre noder i nettverket. Som analysen viser gjentar funn seg fra måned til måned og fra år til år, og enkelte aktører er mer sentrale enn andre. Noder med høy grad av mellomleddssentralitet er tradisjonelt sett aktive bidragsytere i et nettverk der de har kontroll over informasjonsflyten mellom noder. Noden vil befinne seg sentralt i mellom andre aktører, og kunne fungere som en portvokter eller brobygger mellom ulike klynger i nettverket. Analysen viser at beregninger av noders sentralitet enten det er snakk om fartøyer, selskaper eller geografiske noder kan gi verdifull informasjon om nettverk.

Cunningham poengterer at noder med mange registrerte relasjoner til andre kan være et resultat av feil i innsamling av data (Cunningham et al., 2016, s. 144). En svakhet ved beregning av sentralitetsscore i denne oppgaven er at den er påvirket av hvilke fartøy som ligger til kai i samme havn. Sentrale aktører vil derfor kunne endre status dersom kriterier for utvelgelse endres. Det er også viktig å se dette i sammenheng med de kriterier og filter satt for oppgaven. Dersom kriterier for hva som regnes som et avvik i denne oppgaven hadde blitt endret, ville også sentralitetsscore også sannsynligvis bli endret. Ved en sensitivitetsanalyse av datasettet ville man kunnet avdekke dette ved å kontrollere hvordan endring av den satte fartsbegrensningen i filteret ville påvirke resultatene. Dette er ikke blitt gjennomført.

## 8.4 Ser vi en utvikling?

Analysen viser at ved å studere utviklingen over to år er det mulig å si noe om normalsituasjonen samt avvik fra denne. Man kan ved bruk av stordata og SNA studere mønster og sammenhenger for å kartlegge utviklingstrekk. Det er en økning i antall registrete fartøyer og selskaper fra 2014 til 2017. På bakgrunn av et økt antall satellitter fra 2014 til 2017 og måten data lagres på er antallet registreringer betydelig øket mellom de to årene. Dette kunne hatt stor innvirkning på det overordnede resultatet. For den maritime situasjonsbevisstheten er dekningsområdet i 2017 datasettet større, og man får blant annet registreringer på fiskeriaktivitet nord i Barentshavet og rundt Bjørnøya. Denne type aktivitet var ikke mulig å få gode målinger på i 2014. Dette påvirker blant annet nettverkstettheten til hele nettverket av fartøyer og selskaper som vi skal se nærmere på under. Ser vi bort fra en observert endring i trender vedrørende fiskerier, der resultatene fra 2017 viser at nettverkene ikke i like stor grad benytter havner som Ålesund og Tromsø, er resultatene sammenlignbare.

Analysen viser at de mest aktive og sentrale selskapene uavhengig av årstall er *Northern Shipping Company (NSC), Murmansk Shipping Company (MSC), og Sovcomflot (SCF).* Andre selskaper har også sentrale roller i nettverket, men variasjonene hos disse er større med tanke på sentralitet. På bakgrunn av gjentatte stopp i tillegg til samlokalisering med andre fartøyer gjennom begge årene, danner grunnlag for å knytte ekstra oppmerksomhet mot disse. Ser vi til enkeltnoder viser analysen at mønsteret for fartøysnettverket har store likhetstrekk fra det ene året til det andre, til tross for en økning i antall registrerte fartøyer fra 2014 til 2017 på 24%.

## 8.5 En økt maritim situasjonsbevissthet?

Forsvaret må ha selvstendig evne til å drive etteretning for å etablere og vedlikeholde situasjonsforståelse i norske interesseområder (Forsvarsdepartementet, 2016, s. 24). Evne til å skape en maritim situasjonsbevissthet blir i dag utfordret ved at det, på tross av samarbeid på tvers av statlige sektorer, eksisterer begrensede ressurser for å avdekke potensielle avvik. Interesseområdets størrelse, antallet fartøyer som daglig opererer i det, sammen med en kompleks infrastruktur knyttet til næringsvirksomhet, gir oss en utfordring med å prioritere de nasjonale ressursene. Ser vi dette i sammenheng med størrelsen på datasettet i denne oppgaven illustrerer dette informasjonsmengden som må håndteres for å kunne gi et grunnlag for rettidige beslutninger for vår egen politiske og militære ledelse. I lys av kapittel to og tre vil bruk av irregulære kapabiliteter gi mulighet til å skape tvetydighet som også åpner for at

russiske myndigheter kan fornekte kapabilitetens eksistens. Kan SNA bidra til å møte disse utfordringene, og bidra til økt situasjonsbevissthet?

Analysen viser at bruk av stordata og SNA kan være et effektivt «startpunkt» eller utgangspunkt for å øke maritim situasjonsbevissthet, og en metode som potensielt kan gi stor merverdi kombinert med analyse av allerede kjent informasjon. Hovedpoenget her er at stordata og bruk av SNA vil kunne frigjøre kapasitet til å analysere neste nivå i «hierarkiet» for alle involverte aktører. Avviksdeteksjon, å kartlegge puslespillbitene, kan gjøres ved matematiske beregninger og integreres i eksisterende systemer. Dette vil kunne frigjøre sensorkapasitet, mindre ressurser går med til avviksdeteksjon, og vil dermed bidra til mer effektiv utnyttelse av våre begrensede ressurser. Bruk av algoritmer for å avdekke enkelthendelser av interesse vil kunne bidra til felles situasjonsforståelse, og videre forenkling av koordinering og avstemming av situasjonsbevissthet mellom taktisk, operasjonelt og strategisk kommandonivå[13](Forsvarsstaben, 2014, s. 202).

## Situasjonsoppfattelse

Situasjonsoppfattelse av observerte data består av byggeklossene, som settes i en sammenheng, og danner grunnlag for situasjonsforståelse. Dette er en grunnleggende forutsetning for effektiv operativ innsats (Forsvaret, 2015a, s. 43). Den maritime nettverksanalysen benyttet  denne oppgaven viser viktigheten av at involverte aktører, også på tvers av sektorer i samfunnet, er i stand til å anerkjenne muligheten for at en enkelthendelse kan være del av en synkronisert og systematisk utnyttelse av nasjonale sårbarheter. En strategisk målsetting for Russland i et slikt scenario vil være å drive en effektiv desinformasjonskampanje for å forhindre at NATOs artikkel 5 blir utløst (Giles, 2016, s. 43).

Det maritime domenet er en velegnet arena for en opponent som vil operere fordekt eller skjult. Irregulære virkemidler vil som vi har sett gjøre det utfordrende å fastslå om det pågår angrep eller ikke, samt at det også er utfordrende å slå fast hvem som står bak. Observerte data må derfor tolkes som potensielle virkemidler eller hendelser som strekker seg forbi det domenet observatøren[14] selv har ansvar for. Man må få alle involverte i prosessen til

13 Tre nivåer i hierarkiet som utgjør situasjonsbevissthet:
1. Situasjonsoppfattelse av observerte data.
2. Situasjonsforståelse ved integrasjon av data og bevisstgjøring av betydningen for det som skjer.
3. Situasjonsprediksjon innebærer en evne til å forutse hendelser basert på gjenkjenning av tidligere mønster.

14 Eksempel på observatør kan være en representant fra Kystverket, Tollvesenet, Fiskeridirektoratet, Politiet, Hovedredningssentralene, Sjøfartsdirektoratet eller Forsvaret.

å spørre seg selv spørsmål som: *«Kan dette fartøyets adferd, eller denne hendelsen være interessant for noen andre enn meg selv?»* Det vil i så måte være viktig å anerkjenne selv små og tilsynelatende ubetydelige hendelser som et viktig bidrag til den overordnede situasjonsbevisstheten.

SNA kan ved gitte filter og algoritmer fange opp avvik ut fra store mengder data, og presentere sammenhenger på en intuitiv og effektiv måte. Analysene i kapittel 8.1, 8.2, 8.3 og 8.4 har vist at SNA plasserer enkelthendelser i et mønster som kan analyseres og kan gi nettverk en sosial kontekst basert på tolking av matematiske beregninger. Vår evne til å skape situasjonsbevissthet baseres på et begrenset antall ressurser, og derav prioriteringer for hvordan disse skal benyttes for å få forståelse for hva som skjer i det komplekse domenet som våre interesseområder utgjør. Det kan hevdes at man ved bruk av stordata og SNA frigjør sensorkapasitet fra det laveste nivået slik at man selv på taktisk nivå kan tilstrebe økt situasjonsforståelse der man i dag i mange tilfeller observerer enkelthendelser som uavhengige og ubetydelige.

## Situasjonsforståelse

Forsvaret må ha evne til en så tidlig varsling som mulig og kunne etablere og opprettholde situasjonsforståelse på strategisk, operasjonelt og taktisk nivå (Forsvarsdepartementet, 2016, s. 118). For å skape situasjonsforståelse av analysegrunnlaget må enkeltobservasjoner integreres slik at man får en helhetlig forståelse av omgivelsene (Forsvaret, 2015a, s. 133). Men, kompleksiteten i situasjonsbildet kan gjøre det utfordrende å registrere uregelmessigheter, og i tilstrekkelig grad rette beslutningstakers oppmerksomhet mot avvik fra normalsituasjonen. Da er det også utfordrende å oppnå en god situasjonsforståelse av hybride trusler i det maritime domenet. Stavridis sitt syn underbygger dette. Situasjonen i Sør-Kina-havet er overførbar til russiske handlemåter, og vi har sett at sivile fartøyer med eksempelvis ikke-uniformert militært personell, bruk av disse til økt etterretningsvirksomhet eller i kinetiske ikke-attribuerbare virkemidler som sabotasje, kan bli en utfordring.

Evne til å se hendelser og aktiviteter i en sammenheng for å avdekke en hybrid trussel mot Norge på et tidlig tidspunkt vil være av stor viktighet. Mulighet til å identifisere og forstå trusler utgjør grunnlaget for å treffe relevante tiltak (Forsvarsdepartementet, 2016, s. 118). Bruk av felles integrerte systemer som Barents Watch, MARSUR og SafeSeaNet bidrar i dag til at ulike aktører lettere kan se hendelser i sammenheng, utover sitt eget ansvarsområde.

Integrasjon av metoder for maritim nettverksanalyse vil kunne bidra til at situasjonsoppfattelse av observerte data systematiseres av algoritmer og koder. Poenget her er

at bedre utnyttelse av allerede tilgjengelige data vil kunne øke forståelse. Da er det ikke sikkert at svaret for å øke situasjonsbevisstheten ligger i mer ressurser til overvåkning. Ved å koble sammen historiske data som denne oppgaven har tatt for seg og sanntidsbildet vi har, vil SNA kunne bidra til økt situasjonsforståelse. Videre vil metoden som vi har sett i analysen også kunne gi et bilde på sentrale aktører i form av fartøyer, selskaper og geografiske områder og hvilke av disse som innehar sentrale posisjoner. Ved å analysere AIS data kan maritim nettverksanalyse gi oss ny informasjon om hvordan relasjonene mellom ulike noder fortoner seg. Resultatene fra analysen i denne oppgaven viser hvordan analyse av stordata kan integreres for finne sammenhenger og mønster. Ved å sammenligne resultater fra 2014 og 2017 illustreres muligheten for å overvåke utviklingstrekk og endringer i nettverk over tid. Utfordringen med russisk helhetlig tilnærming vil være å skille hendelser med hybrid karakter fra uskyldige hendelser. Som Diesen påpeker vil mønster ofte først kunne kartlegges i ettertid (Diesen, 2018, s. 22).

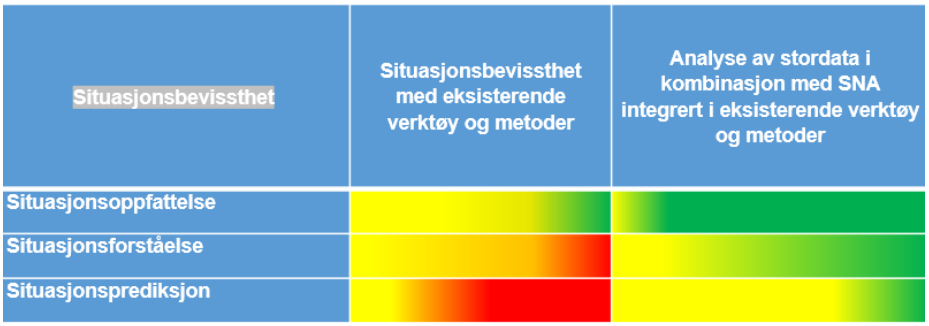
## Situasjonsprediksjon

Situasjonsprediksjon innebærer en evne til å forutse hendelser basert på gjenkjenning av tidligere mønster. Dette nivået bygger på de foregående og omfatter evnen til å forutse hendelser som kan skje i nær fremtid (Forsvaret, 2015a, s. 133).

Analysen i denne oppgaven har vist at man kan bruke stordata og SNA til å beregne mønster, sammenhenger og relasjoner mellom aktører. Det ligger i mørke eller grå nettverks natur at de vil ønske å forbli skjult (Everton, 2012, s. 399). Disse nettverkene kjennetegnes blant annet av at de ofte har evnen til å opprettholde fleksibilitet, og hurtig kunne tilpasse seg endringer (Raab & Milward, 2003, s. 430). Tar vi dette i betraktning vil det være utfordrende å forutse hendelser. På en annen side vil innsikt og forståelse av sentrale aktører, mønster og sammenhenger over tid i det minste kunne bidra til et analytisk grunnlag for forutse hybride trusler basert på historiske data. Videre vil SNA som vi har sett av analysen potensielt kunne frigjøre kapasitet fra de lavere nivåene både hos aktørene og i hierarkiet som utgjør situasjonsbevisstheten. På denne måten vil bruk av stordata og SNA kunne frigjøre ressurser til å opprettholde situasjonsforståelse, samt kunne predikere hendelser i nær fremtid.

Dersom SNA skal kunne benyttes for å øke vår maritime situasjonsbevissthet må vi også være klar over begrensningene til metodene. SNA representerer ikke en «magisk løsning» på utfordringene som representeres av den russiske helhetlige tilnærmingen, men må sees på som et supplement til allerede eksisterende systemer og prosesser (Everton, 2012, s. 365). For å kunne presentere et nyansert og riktig bilde av mulighetene er det også behov for å

se på analysene med forbehold. Nettverksanalysens resultat er styrt av datasettet som analysen bygger på. Avvik fra normalt seilingsmønster ble registret matematisk og er kun avhengig av filter i kodingen av R. Alle avvik er dermed i utgangspunktet registrert. Men, nodene i sosiogrammene og kategorisering av disse nodene i analysedelen risikerer alltid å være mangelfull eller upresise. Dette vil kunne påvirke resultatene. Endringer i dynamiske nettverk som utvikler seg over tid, mangelfulle eller upresise data, avgrensninger og filtrering av datasettet kan alle påvirke resultater (Everton, 2012, s. xxvii). Dette er tilfellet også i denne analysen, hvor eksempelvis kriteriene for hva som er et «fartøy av interesse» får en viktig rolle i hvordan nettverksstrukturene dannes. Dette kan gi en såkalt *confirmation bias*, hvor man ser etter måter å bekrefte ens hypoteser. Svakheter ved AIS data er påpekt tidligere i studien, og har en rekke potensielle feilkilder. Bruk av andre filter og andre algoritmer for identifikasjon av noder kunne gitt andre utslag, og andre beregninger på sentrale aktører i disse nettverkene. Bruk av SNA for å identifisere maritime nettverk er enda i en tidlig fase, og dette påvirker hvor langt det er mulig å dra analysen innenfor rammene av denne studien.




Figur 8.57 Illustrasjon på hvordan stordata og SNA potensielt kan bidra til økt maritim situasjonsbevissthet. Økt kapasitet til evne å oppfatte avvik påvirker situasjonsforståelse i positiv retning, som igjen frigjør kapasitet til å opprettholde denne samt kunne predikere hendelser i nær fremtid basert på tidligere avdekkede mønster og sammenhenger. Illustrasjonen er ikke ment å være en nøyaktig fremstilling av resultater, men en illustrasjon for å oppsummere kapittel 8.5.

Figur 8.57 illustrerer at bedre analyser av allerede innsamlede og tilgjengelige data kombinert med åpne kilder vil kunne «forenkle» det komplekse informasjonsbildet i det maritime domenet. Analysen i denne oppgaven viser at stordata og SNA kan bidra til å identifisere avvik gjennom automatiserte prosesser og bruk av matematiske beregninger gitt i filter og algoritmer. Ser man på historikken (summen av byggeklosser satt i system) vil man for eksempel danne seg et bilde på om en enkelt aktør eller cluster av ulike nettverk har utvist tilsvarende adferd tidligere. Dette kan bidra til at selv sensorer (for eksempel marine-eller kystvaktfartøyer) kan oppnå en økt situasjonsforståelse sammenlignet med dagens verktøy og prosedyrer. Fordelen med dette er at også lavere nivåer i en etat eller organisasjon kan søke å

se sammenhenger som strekker seg ut over det å kun registrere enkelthendelser. Forenklet kan man si at fokuset på situasjonsoppfattelse vil måtte vike for et økt fokus på situasjonsforståelse, der man med dagens systemer og prosedyrer ikke har de samme fortsetninger for dette. Evne til prediksjon kan potensielt øke når man i større grad kan basere disse på mange systematiske historiske observasjoner på avvikende adferd. For å møte maritime hybride trusler ligger altså svaret ikke nødvendigvis i *mer* overvåkning, men i *bedre* utnyttelse av allerede innsamlede data.

## 8.6 Delkonklusjon

For kartlegging av maritime hybride trusler i lys av russisk helhetlig tilnærming har dette kapittelet illustrert hvordan stordata og sosial nettverksanalyse (SNA) som metode kan benyttes til å kartlegge maritime hybride trusler. Gjennom analyse av stordata og bruk av SNA har analysen vist til eksempler på mulige sammenhenger og mønster basert på historiske data. Sentrale aktører i nettverk har blitt identifisert, mønster og sammenhenger er blitt kartlagt, og resultatene er konsistent når man sammenligner 2014 og 2017 data. Mange av de samme fartøyene gjennomfører gjentatte stopp flere steder langs kysten. Avvikene skjer som studien viser, i områder som ikke vurderes som sentral i utførelsen av primæroppgaven, som i de fleste tilfeller er å frakte gods fra A til B.

Ved bruk av algoritmer til analyse av stordata kan kapasitet fra våre begrensede ressurser frigjøres til å kunne fokusere på de to øverste nivåene i det å skape maritim situasjonsbevissthet. Dette gjelder både på taktisk, operasjonelt og strategisk nivå. Men som dette kapittelet har vist, kan man ved å fokusere på maritime nettverks strukturer finne sentrale aktører i form av fartøyer, selskaper og geografiske områder. Ved å benytte stordata og SNA vil man over tid danne et stadig bedre grunnlag for å ikke bare identifisere avvik, men også for å se disse avvikene i en større sammenheng. Dersom bruk av data og metoden for analyse av maritime nettverk benyttes i eksisterende prosesser kan resultatene bidra til en økt situasjonsbevissthet ved at situasjonsoppfattelse og avviksdeteksjon kan håndteres på mer effektive måter.

Men, identifikasjon av avvik som en hybrid trussel eller evne til å forutse signaler om en opptrapping av den helhetlige tilnærmingen kan ikke gjøres ved bruk av SNA alene. Metoden har også svakheter, og kan ikke alene gi alle svar. Benyttet riktig og om mulig integrert i eksisterende systemer og prosesser vil sosial nettverksanalyse kunne bidra til økt situasjonsbevissthet i det maritime domenet, og dermed gi en økt evne til å kartlegge potensielle hybride trusler.

# 9 Konklusjon

«*The international consensus on 'hybrid warfare' is clear, no one understands it, but everyone, including NATO and the European Union, agrees it is a problem» (Cullen & Reichborn-Kjennerud, 2017, s. 3).*

Russisk helhetlig tilnærming til konflikt, ved kombinert bruk av militære, politiske, økonomiske, sivile og informasjonsmessige virkemidler for å undergrave NATO og alliansens partnere har fått økt oppmerksomhet i kjølvannet av krisen i Ukraina[15]. Med bakgrunn i dette har oppgaven analysert sentrale utviklingstrekk i væpnede konflikter og hva som er den dimensjonerende trusselen for Norge. Den russiske helhetlige tilnærmingen til konflikt kjennetegnes, som Diesen påpeker, av at irregulære virkemidler benyttes til fordel for konvensjonelle maktmidler. Utviklingen av krigens karakter er som Gerasimov hevder, at forholdet mellom ikke-militære virkemidler og militære virkemidler i dag er 4:1. Bruk av hybride virkemidler gjør at påvirkning av motpartens vilje og situasjonsforståelse i noen grad erstatter maktanvendelse av fysisk karakter, og gjør det utfordrende å fastslå om det pågår angrep eller ikke, samtidig som det er utfordrende å slå fast hvem som står bak.

Til tross for at det er blitt gjort en rekke forsøk på å sette merkelapp på både begrepet og definisjonen av hybrid krigføring pågår diskusjonen fortsatt. Utfordringen med å komme frem til en felles enighet om hva begrepet faktisk innebærer, fremmer et behov for videre drøfting, noe oppgaven forhåpentligvis bidrar til.

Den helhetlige tilnærmingen gjenspeiles i russisk maritim doktrine, som anerkjenner både russiske militære og sivile fartøyer som en viktig bidragsyter til russiske myndigheters projeksjon av sjømakt. Kinas metoder i Sør-Kina-havet er overførbare til våre interesseområder og russisk handlemåte ifølge Stavridis. I lys av dette vil bruk av mørke eller grå maritime nettverk gjøre det vanskelig å skille uskyldige hendelser fra hendelser med hybrid karakter. I tråd med Mark Galeottis synspunkter har russisk helhetlig tilnærming i det maritime domenet følgende kjennetegn:

1. Villigheten til å gi ikke-kinetiske operasjoner, størst plass.

[15] MPECI

2. Den tette institusjonaliserte forbindelsen med, og bruk av ikke-statlige aktører, selv dem uten åpenbare tilknytninger til Russland.
3. En enhetlig kommandostruktur som i stor grad knytter sammen politiske og militære operasjoner.

Den innledende hypotesen i oppgaven var at norsk evne til å skape tilstrekkelig maritim situasjonsbevissthet, i lys av russisk helhetlig tilnærming til konflikt, ikke er innrettet for å møte hybride trusler i det maritime domenet. Som oppgaven har redegjort for skapes maritim situasjonsbevissthet gjennom sammenstilling av informasjon med bidrag fra ulike aktører i maritim forvaltning. Utveksling av relevant informasjon mellom etater bygger opp under vår nasjonale evne til å drive suverenitetshevdelse og ivaretakelse av samfunnssikkerhet. Hovedutfordringen er å gi tilstrekkelig fokus og prioritere begrensede ressurser mot de delene av det maritime domenet som trenger det til enhver tid. Videre er det utfordringer med å dele relevant informasjon mellom ulike statlige sektorer. Disse faktorene peker på sårbarheter som en hybrid motstander vil kunne utnytte. De begrensede ressursene og kompleksiteten i det totale informasjonsbildet i våre interesseområder gjør at vi må tenke nytt. Svaret ligger kanskje ikke i *mer* overvåkning, men *bedre* og økt utnyttelse av allerede innsamlede og tilgjengelige data.

Hensikten med den maritime nettverksanalysen i denne oppgaven har vært å gi et «proof of concept» for hvordan bruk av stordata og SNA kan øke situasjonsbevisstheten. Gjennom etablering og utvikling av analyseverktøy med tilhørende algoritmer, og en strategi for nettverksmodellering, har studien vist at kartlegging av maritime nettverk kan bidra til å redusere kompleksiteten i det maritime domenet. Store mengder informasjon er blitt systematisert og forenklet ut i fra AIS stordata for årgangene 2014 og 2017. Basert på gitte kriterier for nettverksmodellering har datamaterialet dannet grunnlag for å analysere ulike former for nettverksstrukturer i norske interesseområder. Analyseverktøyet som er utviklet gir oss muligheten til å utlede matematiske beregninger av relasjoner i nettverket ved å analysere grafer bestående av noder som fartøyer, stoppunkter og geografiske områder.

Totalt 156 ulike russiske fartøy og 49 kommersielle og statlige russiske selskaper er identifisert. Sentrale og aktive aktører er blitt identifisert måned for måned. Mønster og sammenhenger er blitt kartlagt basert på historiske data, og resultatene er konsistent når man sammenligner de to årene studien har tatt for seg. Mange av de samme fartøyene gjennomfører gjentatte stopp flere steder langs kysten, og det er identifisert avvik i forbindelse med både egne og allierte øvelser i tillegg til uregelmessigheter før og under

eksempelvis øvelsen Zapad i 2017. Avvikene involverer i stor grad russiske kommersielle fartøyer. Som analysen viser, opptrer disse med uregelmessigheter i områder som ikke vurderes som sentral i utførelsen av deres primæroppgave, som i de fleste tilfeller er å frakte gods fra A til B.

Ved bruk av beregninger av relasjoner i nettverk og bruk av algoritmer til analyse av stordata kan kapasitet fra våre begrensede ressurser frigjøres til å kunne fokusere på situasjonsforståelse og prediksjon av nær fremtid. Man kan ved å fokusere på maritime nettverksstrukturer finne sentrale aktører i form av fartøyer, selskaper og geografiske områder. Ved å benytte stordata og SNA vil man over tid danne et bedre og bedre grunnlag for å ikke bare identifisere avvik, men å se disse avvikene i en større sammenheng. Studien viser at stordata og SNA kan bidra til økt forståelse av dynamikken i slike nettverk, og bidra til å identifisere hvordan man kan tilnærme seg disse for å unngå at de utnytter sine kapasiteter. Dersom bruk av data og metoden for analyse av maritime nettverk benyttes i eksisterende prosesser kan resultatene bidra til en økt situasjonsbevissthet ved at situasjonsoppfattelse og avviksdeteksjon håndteres mer effektivt.

Identifikasjon eller prediksjon av hybride trusler kan dog ikke gjøres ved bruk av SNA alene. Oppgaven tar utgangspunkt i analyse av historiske AIS-data. Studien viser at det finnes feilkilder i AIS-systemet, som i tillegg til tekniske feil ofte kan tilskrives bevisste eller ubevisste menneskelige feil. Feilkildene vil kunne påvirke datasettet som er omhandlet i denne studien. Nytteverdien av metoden må alltid sees i sammenheng med annen beslutningsstøtte, og ikke alene stå som beslutningsgrunnlag.

Studien viser at SNA er et kraftfullt verktøy når det anvendes riktig. Den endelige konklusjonen er derfor at stordata og sosial nettverksanalyse kan bidra til økt maritim situasjonsbevissthet forutsatt at det benyttes riktig og som et supplement til eksisterende prosesser og systemer. Det anbefales derfor å forske videre på problemstillinger knyttet til denne tematikken, for å vurdere hvorvidt SNA også i andre sammenhenger kan bidra til økt operativitet.

## 9.1 Anbefalt videre forskning

Oppgaven tar for seg en problemstilling som i liten grad er belyst tidligere, og det står igjen ubesvarte spørsmål som bør studeres videre. Det anbefales at fremtidige studier ser på hvordan metodene fra SNA kan integreres i eksisterende systemer og infrastruktur, og hvilke tekniske løsninger og analysekapasiteter vi eventuelt trenger for å iverksette analyse av maritime hybride trusler i sanntid.

Bruk av stordata og SNA i et totalforsvarsperspektiv bør også studeres nærmere. Kan SNA integreres på et operasjonelt nivå, og bidra til økt situasjonsbevissthet også i andre sektorer og forsvarsgrener? Hvem som skal ha ansvaret for kartlegging, registrering og deling av relevant informasjon i et totalforsvarsperspektiv bør analyseres nærmere. Selv om denne studien peker i den retningen, er det ikke gitt at dette ansvaret bør ligge hos FOH.

I ytterste konsekvens vil situasjonsforståelse av maritime nettverk i våre interesseområder, uavhengig av nasjonalitet, være avgjørende også i en situasjon der en opponent trapper opp. I en krise eller væpnet konflikt vil sentrale aktører i skjulte maritime nettverk, under gitte forutsetninger, kunne bli lovlige militære mål. Videre forskning bør derfor se på bruk av stordata og SNA eventuelt kan benyttes i «targeting-prosessen» på operasjonelt nivå, for å vurdere om metoden også bør integreres i syklusen som velger ut og prioriterer militære mål.

# 10 Litteraturliste


Aftenposten. (2007, 11. desember 2007). Norge leverte protest til Russland. *Aftenposten*. Hentet fra http://www.aftenposten.no/norge/i/rWrwk/Norge-leverte-protest-til-Russland

Balkundi, P. & Harrison, D. A. (2006). Ties, leaders, and time in teams: Strong inference about network structure's effects on team viability and performance. *Academy of Management Journal, 49*(1), 49-68.

Bartles, C. K. (2016). Getting Gerasimov right.(RUSSIAN VIEW). *Military Review, 96*(1), 30.

Blix, T. A. (2014). FFI-rapport 2014/02041: Maritimt samarbeid innen EU, landene rundt polområdet, og Norges tilslutning til de ulike organisasjonene og prosjektene. I. Kjeller: Forsvarets forskningsinstitutt FFI. Hentet fra http://www.ffi.no/no/Rapporter/14-02041.pdf

Borgatti, S. P. & Foster, P. C. (2003). The network paradigm in organizational research: A review and typology. *Journal of management, 29*(6), 991-1013.

Busch, T. (2013). *Akademisk skriving for bachelor-og masterstudenter* Fagbokforl.

Connolly, D. R. (2017). *Towards a Dual Fleet?: The Maritime Doctrine of the Russian Federation and the Modernisation of Russian Naval Capabilities*. http://www.ndc.nato.int/news/news.php?icode=1061: NATO Defense College. Hentet fra http://www.ndc.nato.int/news/news.php?icode=1061

Creswell, J. W. (2014). *Research design : qualitative, quantitative, and mixed methods approaches* (4th ed.; International student ed. utg.). Los Angeles, Calif: SAGE.

Cullen, P. & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare* NUPI.

Cunningham, D., Everton, S. & Murphy, P. (2016). *Understanding dark networks : A strategic framework for the use of social network analysis*. Rowman & Littlefield Publishers.

Davis, A. (2015). *Morskaya Doktrina Rossiyskoy Federatsii [Maritime doctrine of the Russian Federation]*. Hentet fra https://usnwc.edu/Research-and-Wargaming/Research-Centers/Russia-Maritime-Studies-Institute

De Nooy, W., Mrvar, A. & Batagelj, V. (2018). *Exploratory social network analysis with Pajek* Cambridge University Press.

Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt. I. Kjeller: Forsvarets forskningsinstitutt FFI. Hentet fra http://rapporter.ffi.no/rapporter/18/00080.pdf

Eric, R. D., Colin, J. C., Jason, K. B. & Wayne, M. G. (2017). *A cross-validation-based approach for delimiting reliable home range estimates*.

Erickson, A. S. (2016). America's security role in the South China Sea. *Naval War College Review, 69*(1), 7.

Everton, S. F. (2012). *Disrupting dark networks* Cambridge University Press.

FalckNutec. (2014). GOC General Operators Certificate. I(06. januar 2014 utg.): Falck Nutec.

FD/JD. (2015). *Støtte og samarbeid : En beskrivelse av totalforsvaret i dag*. Oslo: Forsvarsdepartementet.

Forsvaret. (2015a). *Forsvarets doktrine for maritime operasjoner*. Bergen: Forsvaret.

Forsvaret. (2015b). *Verden i endring : Forsvarets årsrapport 2014*. Oslo: Forsvaret.

Forsvaret. (2017). Øvelse Joint Viking 2017. Hentet 02. nov 2018 2018 fra https://forsvaret.no/jointviking
Forsvarsdepartementet. (2015). *Et felles løft : ekspertgruppen for forsvaret av Norge*. Oslo: Forsvarsdepartementet.
Forsvarsdepartementet. (2016). *Kampkraft og bærekraft : langtidsplan for forsvarssektoren*. Oslo: Departementet.
Forsvarsstaben. (2014). *Forsvarets fellesoperative doktrine*. Oslo: Forsvarsstaben.
Freeman, L. C. (1979). Centrality in social networks: Conceptual Clarification. *Social networks, 1*(3), 215-239.
Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars & Insurgencies, 27*(2), 282-301. https://doi.org/10.1080/09592318.2015.1129170
Giles, K. (2016). Russia's 'New'Tools for Confronting the West. *Continuity and Innovation in Moscow's Exercise of Power*.
Golbeck, J. (2013). *Analyzing the social web* Newnes.
Hicks, K. (2018). *Contested Seas, Maritime Domain Awareness in Northern Europe* (CSIS International Security Program). Center for Strategic & International Studies. Hentet fra https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180328_MetrickHicks_ContestedSeas_Web.pdf?AaSGbCYstp_dVE22M_UODVuJvVS0_mkM
IMO. (2015). *A29/Res.1106. Revised guidelines for the onboard operational use of shipborne automatic identification systems (AIS)*. International Maritime Organization.
IMO. (2017). *Resolution A.1117(30). IMO Ship Identification Number Scheme*. International Maritime Organization.
Joansen, P. A. (2018). Dette bildet skal vise at Putins mektige venner dro på hemmelig fisketur i Norge. Her er årsakene til at det kan bli en stor skandale. *Aftenposten*. Hentet fra https://www.aftenposten.no/verden/i/J1xg16/Dette-bildet-skal-vise-at-Putins-mektige-venner-dro-pa-hemmelig-fisketur-i-Norge-Her-er-arsakene-til-at-det-kan-bli-en-stor-skandale
Johnson, R. (2018). Hybrid War and Its Countermeasures: A Critique of the Literature. I(Vol. 29, s. 141-163): Routledge.
Jones, C. D. (2003). Soviet military doctrine as strategic deception: An offensive military strategy for defense of the socialist fatherland. *The Journal of Slavic Military Studies, 16*(3), 24-65. https://doi.org/10.1080/13518040308430567
Kadushin, C. (2012). *Understanding social networks: Theories, concepts, and findings* OUP USA.
Kofman, M. (2016). Russian hybrid warfare and other dark arts. *War on the Rocks, 11*. Hentet fra https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/
Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections, 24*(3), 43-52.
Kremidas-Courtney, C. (2018). Countering Hybrid Threats in the Maritime Environment. Hentet fra cimsec-org/countering-hybrid-threats-in-the-maritime-environment/36553
Kystverket. (2017a). AIS-satellittar. Hentet 07. nov 2018 2018 fra https://www.kystverket.no/Maritime-tjenester/Meldings--og-informasjonstjenester/AIS/AISSat-1-og-AISSat-2/
Kystverket. (2017b). *Årsmelding 2017*. Hentet fra https://www.regjeringen.no/contentassets/dfe89791d3744379b5242d79975ae528/arsmelding-2017-for-kystverket---web.pdf
Kystverket. (2018). *Status 2018*. Hentet fra www.kystverket.no/Om-Kystverket/Brosjyrer-skjema-og-andre-publikasjoner/Brosjyrer2/status/

Lanestedt, G. (2016). Stordata og kunnskapsbasert forvaltning. *Stat & styring*, (02), 52-54.
Lasconjarias, G. & Larsen, J. A. (2015). *NATO's Response to Hybrid Threats* NATO Defense College, Research Division.
Linnarsson, G. (2015). En prestandajämförelse mellan databaskopplingar i R. I *A performance Comparision between database connections in R*.
McDermott, R. N. (2016). Does Russia have a Gerasimov doctrine? *Parameters, 46*(1), 97.
Murphy, M., Hoffman, F. G. & Schaub, G. (2016). *Hybrid Maritime Warfare and the Baltic Sea Region* Centre for Military Studies, University of Copenhagen.
NATO. (2006). *Riga Summit Declaration*. NATO. Hentet fra http://www.nato.int/docu/pr/p06-150e.htm
NATO. (2014a). More than just information gathering. Hentet 15. oktober 2018 fra https://www.nato.int/cps/en/natohq/news_110351.htm?selectedLocale=en
NATO. (2014b, 26. Sep 2016). Wales Summit Declaration. Hentet 05. Aug 2018 2018 fra www.nato.int/cps/ic/natohq/official_text_112964.htm
NATO. (2015). Keynote speech by NATO SECGEN Jens Stoltenberg. Hentet 05 May 2018 fra https://www.nato.int/cps/ic/natohq/opinions_118435.htm
NATO. (2017a). SNMG-1 visits Trondheim. Hentet 2018 fra https://mc.nato.int/media-centre/news/2017/standing-nato-maritime-group-one-visits-trondheim.aspx
NATO. (2017b). ZAPAD 2017 and Euro-Atlantic security. Hentet 10. november 2018 fra https://www.nato.int/docu/review/2017/also-in-2017/zapad-2017-and-euro-atlantic-security-military-exercise-strategic-russia/EN/index.htm
NEAFC. (2018). Hentet 04. november 2018 2018 fra https://www.neafc.org
NROF. (2018). *Pro Patria - Militærfaglig magasin, Nr. 03/2018*.
Perliger, A. & Pedahzur, A. (2011). Social Network Analysis in the Study of Terrorism and Political Violence. *APSC, 44*(1), 45-50. https://doi.org/10.1017/S1049096510001848
Porter, W., Warren, C. & Schroeder, R. (2018). Mapping Dark Maritime Networks.
PST. (2018). Trusselvurdering 2018. Hentet 13. oktober 2018 2018 fra https://www.pst.no/trusselvurdering-2018/
R-Project. (2018). The R Project for Statistical Computing. Hentet 24. september 2018 fra https://www.r-project.org/about.html
Raab, J. & Milward, H. B. (2003). Dark networks as problems. *Journal of public administration research and theory, 13*(4), 413-439.
Regjeringen. (2014). *Norsk økonomisk sone*. regjeringen.no: Regjeringen. Hentet fra https://www.regjeringen.no/no/tema/mat-fiske-og-landbruk/fiskeri-og-havbruk/rad-1/fiskeri-ny/rydde-internasjonalt/norges-okonomiske-sone/id434515/
Rstudio. (2018). Leaflet for R. Hentet 20. november 2018 fra https://rstudio.github.io/leaflet/
Seely, R. (2017). Defining Contemporary Russian Warfare: Beyond the Hybrid Headline. *The RUSI Journal, 162*(1), 50-59.
Sergunin, A. & Konyshev, V. (2017). Russian military strategies in the Arctic: change or continuity? *European Security, 26*(2), 171-189. https://doi.org/10.1080/09662839.2017.1318849
Simmel, G. (1906). The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology, 11*(4), 441-498. https://doi.org/10.1086/211418
Sovcomflot. (2018). SCF homepage. Hentet 09. oktober 2018 2018 fra http://sovcomflot.ru/en/investors/corporate_governance/boardofdirectors/item1469.html
Stavridis, J. (2016). Maritime Hybrid Warfare Is Coming. *US Naval Institute Proceedings* (s. 30-33).
Stavridis, J. (2018). E-post fra Admiral James Stavridis. I.

Vivento. (2015). *Kartlegging og vurdering av stordata i offentlig sektor*. Oslo: Kommunal- og moderniseringsdepartementet. Hentet fra https://www.regjeringen.no/no/dokumenter/kartlegging-og-vurdering-av-stordata-i-offentlig-sektor/id2478539/

Vogel, K. P. & Rosenberg, M. (2018). U.S. Agents Tried To Turn Oligarch Into an Informer.(National Desk). I(s. A1).

Wallace, T. & Mesko, F. (2013). *The Odessa Network: Mapping Facilitators of Russian and Ukrainian Arms Transfers* C4ADS.

Windward. (2014). Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea. Hentet fra https://www.arbitrage-maritime.org/fr/Gazette/G36complement/Windward.pdf

Østvang, K. & Kemp, I. (2007, 12. desember 2007). Stort oljeutslipp i Nordsjøen. *Aftenposten*. Hentet fra http://www.aftenposten.no/norge/i/zrq1K/Stort-oljeutslipp-i-Nordsjøen

# 11 Vedlegg

A. Godkjenning fra NSD

# 11.1 Vedlegg A – Godkjenning fra NSD

Palle Ydstebø
Postboks 800, Postmottak
2617 LILLEHAMMER

Vår dato: 16.07.2018 Vår ref: 61224 / 2 / AMS Deres dato: Deres ref:

## Vurdering fra NSD Personvernombudet for forskning § 31

Personvernombudet for forskning viser til meldeskjema mottatt 21.06.2018 for prosjektet:

| | |
|---|---|
| *61224* | *Dark Maritime Networks i norske interesseområder: Konsekvenser for Forsvaret og Totalforsvaret.* |
| *Behandlingsansvarlig* | *Forsvarets høgskole, ved institusjonens øverste leder* |
| *Daglig ansvarlig* | *Palle Ydstebø* |
| *Student* | *Stian Schnelle* |

### Vurdering

Etter gjennomgang av opplysningene i meldeskjemaet og øvrig dokumentasjon finner vi at prosjektet er meldepliktig og at personopplysningene som blir samlet inn i dette prosjektet er regulert av personopplysningsloven § 31. På den neste siden er vår vurdering av prosjektopplegget slik det er meldt til oss. Du kan nå gå i gang med å behandle personopplysninger.

### Vilkår for vår anbefaling

Vår anbefaling forutsetter at du gjennomfører prosjektet i tråd med:

- opplysningene gitt i meldeskjemaet og øvrig dokumentasjon
- vår prosjektvurdering, se side 2
- eventuell korrespondanse med oss

Vi forutsetter at du ikke innhenter sensitive personopplysninger.

### Meld fra hvis du gjør vesentlige endringer i prosjektet

Dersom prosjektet endrer seg, kan det være nødvendig å sende inn endringsmelding. På våre nettsider finner du svar på hvilke endringer du må melde, samt endringsskjema.

### Opplysninger om prosjektet blir lagt ut på våre nettsider og i Meldingsarkivet

Vi har lagt ut opplysninger om prosjektet på nettsidene våre. Alle våre institusjoner har også tilgang til egne prosjekter i Meldingsarkivet.

### Vi tar kontakt om status for behandling av personopplysninger ved prosjektslutt

*Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.*

Ved prosjektslutt 26.11.2018 vil vi ta kontakt for å avklare status for behandlingen av personopplysninger.

Se våre nettsider eller ta kontakt dersom du har spørsmål. Vi ønsker lykke til med prosjektet!

Katrine Utaaker Segadal

Anne-Mette Somby

Kontaktperson: Anne-Mette Somby tlf: 55 58 24 10 / anne-mette.somby@nsd.no

Vedlegg: Prosjektvurdering
Kopi: Stian Schnelle, sschnelle@fhs.mil.no