Fra gråsonen til hybridkrig: Utfordringer for deteksjon i et norsk perspektiv

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Høst 2017

FORFATTER:

Svend Arne Myhre

VEILEDER:

Paul Magnus Hjertvik Buvarp

TITTEL PÅ MASTEROPPGAVE:

Fra gråsonen til hybridkrig: deteksjon av koordinerte flerdimensjonale trusler i et norsk perspektiv

EMNEORD/STIKKORD: Hybride trusler, scenario, risiko, etterretning, krisehåndtering, HRO, systemfeil, påvirkningsoperasjoner, digitale trusler, sabotasje

SIDETALL: 84

STAVANGER ……20. november 2017…….

DATO/ÅR

Innholdsfortegnelse

Forkortelser ..... **iv**

Sammendrag ..... **v**

Forord ..... **vi**

1. Innledning **1**

1.1 Bakgrunn **1**

1.2 Problemstilling og forskningsspørsmål **3**

1.1.1 Disposisjon 4

1.3 Avgrensninger **4**

1.4 Kontekst **6**

2. Arbeidsform og metoder **10**

2.1 Forskningsdesign **10**

2.2 Metode **12**

2.2.1 Litteraturstudie 13

2.2.2 Morfologisk analyse og scenarier 15

3. Teoretiske perspektiv **17**

3.1 Sikringstiltak **18**

3.1.1 Risiko og trussel, sikkerhet og usikkerhet 18

3.1.2 Krisehåndtering og etterretning 26

3.1.3 Å gjenkjenne trusselen 31

3.1.4 Delkonklusjon 37

3.2 Hybride trusler **39**

3.2.1 Definisjon 39

3.2.2 Sentrale trekk ved hybride trusler 41

3.2.2 Beslektede begreper 46

3.2.3 Delkonklusjon 49

4. Resultater/empiri **50**

4.1 Morfologisk analyse **50**

4.1.1 Parametere og parameterverdier 50

4.1.2 Morfologisk rom 62
4.1.3 Syntesefase 63
4.1.4 Løsningsrom 65
4.2 Scenarioer 66
4.2.1 Scenario 1: "Kamp om sannheten og ressursene" 66
4.2.2 Scenario 2: "Sivile inngrep, aktiv infiltrasjon" 67
4.2.3 Scenario 3: "Militære trusler" 69

5. Drøfting 69
5.1 Deteksjon av separate hendelser i scenarioene 70
5.1.1 Etterretningsvirksomhet 70
5.1.2 Trusler i det digitale rom 72
5.1.3 Informasjonsoperasjoner 74
5.1.4 Stedfortredergrupper og voldelige aksjoner 75
5.1.5 Konvensjonell militær operasjon 76
5.1.6 Sabotasje mot drikkevann 76
5.2 Deteksjon av koordinering 77
5.2.1 Trusselaktørens intensjoner 78
5.2.2 Tvetydig trussel 78
5.2.3 Hybride trusler som "krypende kriser" 81
5.2.4 Befolkningssentrisk trussel 82

6. Konklusjon 83

7. Litteraturliste 85

8. Vedlegg 107
Vedlegg A: Norske offentlige sikkerhetsinsitusjoner 107
Vedlegg B: Hybridbegrepets historie og innhold 108
Vedlegg C: Konsistensmatrise 111

Forkortelser

A2AD	Anti-Access/Area Denial
CIMIC	Civilian-military Cooperation
CNA	Computer Network Attack
CNE	Computer Network Exploitation
DGF	Digitalt grenseforsvar
DSB	Direktoratet for samfunnssikkerhet og beredskap
E-tjenesten	Etterretningstjenesten
FCKS	Felles Cyberkoordineringssenter
FD	Forsvarsdepartementet
FKTS	Felles kontraterrorsenter
FSJ	Forsvarssjefen
FST	Forsvarsstaben
GMA	General Morphological Analysis
HRO	High Reliability Organization
OED	Olje og energidepartementet
POD	Politidirektoratet
HRS	Hovedredningssentralen
JBD	Justis- og beredskapsdepartementet. Før 2009: Justis- og politidepartementet (JPD)
KRU	Koordinerings- og rådgivingsutvalget for etterretnings-, overvåkings- og sikkerhetstjenestene
KSE	Krisestøtteenheten
UD	Utenriksdepartementet
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets sikkerhetsråd
NorCERT	Norway Computer Emergency Reponse Team (NSM)
PST	Politiets sikkerhetstjenest
RSU	Regjeringens sikkerhetsutvalg
SCADA	Supervisory Control And Data Acquisition
SITSEN	Forsvarets situasjonssenter
VDI	Varslingsnettverk for Digital Infrastruktur

Sammendrag

Problemstillingen for oppgaven er å identifisere aspekter ved hybride trusler skaper særlige utfordringer for norske offentlige sikkerhetsinstitusjoners deteksjon av om trusselen er koordinert av en statlig aktør som ønsker å påvirke eller destabilisere. Teori fra safety-området og etterretningsstudier bidrar til svar på problemstillingen gjennom å vise hvordan systemfeil (etterretningsfadeser) kan skje i komplekse systemer, og hvordan disse feilkildene kan motvirkes. Gjennom morfologisk analyse etableres en modell for hybride trusler som danner grunnlag for tre scenarioer. Scenarioene beskriver hvordan en hybrid trussel kan se ut. Disse drøftes i forhold til de norske sikkerhetsinstitusjonenes muligheter og begrensninger slik dette fremkommer i ugraderte kilder for å vurdere mulighetene for å detektere enkelthendelsene. Evne til deteksjon i det digitale rom og evne til å analysere og varsle om påvirkningsoperasjoner fremstår som de største manglene. Svaret på hovedspørsmålet om evnen til å detektere at en trussel er koordinert er at dette er komplisert, men ikke umulig, gitt de rette kapasitetene og god kommunikasjon mellom operativt og strategisk nivå både i normal- og krisesituasjoner for å etablere en korrekt situasjonsforståelse som igjen skaper grunnlag for gode beslutninger. God oversikt over egne sårbarheter og sikring av kritisk infrastruktur vil også bidra til bedre forståelse av trusselen.

Forord

Denne masteroppgaven markerer slutten på tre år med studier ved siden av jobb og familieliv. Det har vært ensomme kvelder og helger foran dataskjermen, en del svette, og kanskje noen tårer. Men mest av alt sitter jeg igjen med følelsen av å være privilegert gjennom at jeg har fått lov av familie og arbeidsgiver til å bruke all denne tiden på å sette meg inn i temaer jeg er opptatt av, og til å nok en gang å bli påminnet om hvor mye jeg ikke vet. Oppgaven representerer selvsagt bare en del av alt arbeidet som er gjort. Mye er lest, mye er prøvd og forkastet, og mye er lært. Min dyktige og vennlige veileder på FFI, Paul Magnus Hjertvik Buvarp, fortjener den største takken for å gi meg retning, kritikk, gode råd og oppmuntring. Dernest min kone og datter for deres tålmodighet med og støtte til en stadig mer nevrotisk deltidsstudent. Tusen takk! Alle feil og mangler som gjenstår tar jeg selvfølgelig på egen kappe.

Svend Arne Myhre

20. november 2017

1. Innledning

1.1 Bakgrunn

Etter den Kalde krigen har trusselbildet utviklet seg i retning av å bli mer usikkert og dynamisk. Det bipolare systemet bestående av to supermakter er borte, og i stedet er langt flere stater globalt involvert i å regulere internasjonale forhold. Fra å håndtere kjente trusler (en hovedsakelig militær trussel fra Sovjetunionen) står Vesten overfor ulike former for risiko som er grenseoverskridende, asymmetriske, komplekse og uforutsigbare, og sikkerhetsinstitusjonenes oppgave handler i større grad om å avverge og forberede samfunnet for ukjente katastrofer. Regionale forhold truer i større grad internasjonal fred og sikkerhet, og ikke-statlige aktører utnytter regionale konflikter og usikkerhet (Dunn Cavelty og Mauer 2009:127, Rathmell 2002:91). Tid og rom er komprimert gjennom globalisering og IKT-revolusjonen. Mennesker, våpen, giftstoffer, narkotika, kunnskap og idéer kan raskt forflytte seg over grenser (Friedman 2005). Trusselbildet vi står overfor er med andre ord preget av kompleksitet og usikkerhet, samtidig som geografisk avstand spiller en stadig mindre rolle (Dunn Cavelty og Mauer 2009:128).

Begrepet hybridkrig ble først tatt i bruk av amerikanske militære analytikere på begynnelsen av 2000-tallet for å beskrive trusselen mot konvensjonelle styrker fra opprørsbevegelser som benytter en blanding av moderne våpensystemer, geriljataktikk og ukonvensjonell organisering. Tsjetsjenske opprørere og Hezbollah ble brukt som eksempler, og hybridkrig ble beskrevet som en form for krig der skillene mellom krig og fred og stridende og ikke-stridende er utydelige (Rinelli og Duyvesteyn 2017:19-21). Etter Russlands anneksjon av Krym og intervensjonen i Donbass ble også den russiske fremgangsmåten her definert som ”hybrid”, gjennom at her så man en statlig aktør som integrerte alle statens maktmidler, militære og ikke-militære, for å oppnå sine strategiske målsetninger (Reichborn Kjennerud og Cullen 2016:2).

Hybridkrig og hybride trusler er omstridte begreper i den akademiske litteraturen. Et argument som ofte forekommer er at krigsbegrepet blir utvannet dersom man setter merkelappen *krig* på ulike former for anvendelse av staters maktmidler. Det debatteres også om dette virkelig er en separat form for konflikt og om det er noe nytt (Renz og Smith 2016:13, Kofman og Rojanski

2015). Historisk kan det påvises eksempler på koordinert bruk av konvensjonelle og ikke-konvensjonelle virkemidler i de germanske stammenes motstand mot romerske legioner i det første århundret e.Kr., under den amerikanske revolusjonen, den fransk-prøyssiske krigen og nazi-Tysklands anneksjon av Østerrike (Murray og Mansoor 2012, Neville 2015).

En hybrid trussel handler om en motstanders vilje og evne til å benytte en kombinasjon av åpenlyse og fordekte militære og ikke-militære virkemidler. En hybrid trussel kan manifestere seg i en mer eller mindre åpen konflikt. I slike tilfeller benytter media og faglitteratur gjerne begrepet hybridkrig. Her vil fortrinnsvis begrepet *hybride trusler* benyttes og *hybridkrig* der hvor det refereres til en væpnet konflikt som for eksempel i Ukraina, eller der hvor kildene spesifikt referer til hybridkrig. Dette reflekterer at hovedfokus ligger på den krevende krisefasen der en væpnet konflikt ennå ikke har brutt ut.

Begrepene hybridkrig og hybride trusler kritiseres for å være dårlig definert. De misforstås og feiltolkes, og de brukes om hverandre, i tillegg til en rekke andre beslektede begrep med mer eller mindre overlappende innhold (Rinelli og Duyvesteyn 2017:19-21). Felles for truslene denne oppgaven fokuserer på er at de er utformet slik at de holder seg under terskelen for krig. Truslene er av en strategisk natur, og er gjerne rettet mot sivilbefolkningen som et "indirekte mål" for å påvirke politiske beslutninger. De er flerdimensjonale i den forstand at militære, politiske, informasjonsmessige, økonomiske og fordekte virkemidler benyttes på en koordinert måte. Effekten vil være et trusselbilde som fremstår som tvetydig, noe som gjør det vanskeligere å reagere for den som utsettes for trusselen.

Den endrede sikkerhetspolitiske konteksten etter den Kalde krigen gjør det like vel relevant og interessant å bruke hybridbegrepet som analytisk utgangspunkt. Flere rammefaktorer er endret, som en globalisert økonomi, 24/7-nyhetsdekning forsterket av sosiale medier og en avtagende appetitt blant vestlige befolkninger på å støtte militære operasjoner som kan medføre tap av liv i stor målestokk (Galeotti 2016b:297). Dermed ser konflikter i dag annerledes ut, og det kan se ut som om gamle virkemidler i dag benyttes på nye og oppfinnsomme måter for å legge press på motstandere i alle faser av konfliktspekteret og oppnå politiske mål på en raskere og tidvis skitnere måte enn tidligere (Lasconjarias og Larsen 2015:1).

Siden hybride trusler kan forekomme både i fred, krise og krig er temaet relevant ikke bare fra et statssikkerhets- men også et samfunnssikkerhetsperspektiv. Informasjonsoperasjoner, sabotasje og økonomisk krigføring rettes direkte mot den sivile befolkningen for å svekke motstandsviljen, utnytte konflikt mellom folkegrupper eller påvirke politiske prosesser i demokratiske samfunn (Rinelli og Duyvesteyn 2017:32).

"Deteksjon" og "koordinering" er de viktigste nøkkelordene i denne oppgaven. Deteksjon av hybride trusler handler om hvordan norske myndigheter ved hjelp av sine sikkerhetsinstitusjoner i Justis- og Forsvarssektoren, ofte i samarbeid med sivile virksomheter, kan forstå at tilsynelatende separate uønskede hendelser faktisk er del av en koordinert operasjon med utgangspunkt i en annen stat som har en politisk intensjon om å oppnå visse strategiske målsetninger. For å oppnå deteksjon må man forstå normalsituasjonen og etablere relevante indikatorer for å gjøre det mulig å fange opp svake signaler om at en trussel kan være i ferd med å manifestere seg, og den eventuelle trusselen må erkjennes av beslutningstagere: *In the case of hybrid threat warning, indicators and monitoring are the most important basis for decision-making* (Mažeikis 2017:7).

1.2 Problemstilling og forskningsspørsmål

Målet med oppgaven er å undersøke hvilke utfordringer norske offentlige sikkerhetsinstitusjoner står overfor når det gjelder å detektere en koordinert hybrid trussel fra en statlig aktør, og ikke en rekke ikke-relaterte hendelser. Hva hindrer oss i å "forvente det uventede"?

<u>Problemstilling:</u> Hvilke aspekter ved hybride trusler skaper særlige utfordringer for norske offentlige sikkerhetsinstitusjoners deteksjon av om trusselen er koordinert?

Viktige forskningsspørsmål til de ulike scenariene og drøftingen av dem vil være:

- Hvilke aktører er involvert i indikasjon og varsling? Hva er deres ansvarsområder? Hvordan samarbeider de?
- I hvilken grad er norske sikkerhetsinstitusjoner i stand til å detektere de enkelte elementene som inngå i en hybrid trussel?

- I hvilken grad samsvarer norske myndigheters trusselpersepsjon (slik den kommer til uttrykk i ugraderte risiko- og trusselvurderinger) med hybride trusler slik de fremkommer i scenarioene?

1.1.1 Disposisjon

Resten av kapittel 1 omfatter avgrensninger som er gjort i arbeidet med oppgaven, samt en beskrivelse av det norske systemet for krisehåndtering på strategisk nivå. Kapittel 2 gjør rede for forskningsdesign og metoder som er benyttet. Kapittel 3 er en gjennomgang av teori knyttet til på den ene siden sikringstiltak, på den andre siden hybridbegrepets innhold. Teoribidragene er hentet både fra etterretningsstudier og fra studier basert på utilsiktede hendelser som industriulykker for en mest mulig helhetlig, *all hazards*, tilnærming. Den morfologiske analysen og scenarioene utgjør kapittel 4 (empiri), mens resultatene av analysen drøftes i relasjon til problemstillingen og teorien i kapittel 5, før resultatene oppsummeres til slutt.

1.3 Avgrensninger

Tilgjengelig tid og tematikkens omfang har naturlig nok gjort det nødvendig å gjøre en rekke avgrensninger og utelate annen interessant tematikk som har dukket opp underveis i arbeidet. Oppgaven vil ikke fokusere nevneverdig på hvordan en hybrid trussel ville blitt håndtert eller respondert på, men på fasen som kommer forut for en uønsket hendelse (dermed betraktes deteksjon som et sannsynlighetsreduserende tiltak), og ikke den konsekvensreduserende fasen. Siden hybride trusler i fremtiden bare vil bli mer komplekse og uforutsigbare i fremtiden, peker enkelte analytikere (Hartmann 2017:2) på viktigheten av å etablere mer resiliens eller robusthet. Resiliens beskriver et samfunns evne til å tåle og håndtere store hendelser, gjenopprette viktige funksjoner etter at hendelser har funnet sted, og om nødvendig tilpasse seg til endrede forutsetninger (Justis- og beredskapsdepartementet 2016:31). Diskusjonen rundt resiliens, som primært handler om konsekvensreduserende tiltak vil ikke drøftes detaljert her[1].

[1] På grunn av økende avhengigheter på tvers av landegrensene kan resiliens heller ikke være et eksklusivt nasjonalt anliggende. Hamilton (2017) anbefaler en proaktiv tilnærming (forward resilience) der allierte og partnere proaktivt deler informasjon og etterretninger, strategier og operative prosedyrer for å håndtere hybride trusler. Tiltak for å bygge resiliens, for eksempel NATOs *Seven Baseline Requirements*, være relevante for å detektere trusler (Meyer-Minnemann 2017)

En sentral del av oppgaven blir å klarlegge hva som utgjør en hybrid trussel med det formål å inkludere relevante elementer i den videre analysen. En mer detaljert fremstilling av historikken rundt selve begrepet er inkludert i vedlegg B.

"Deteksjon" i denne konteksten er ikke bare at en virksomhet oppfanger at de er rammet av et cyberangrep. Det handler om hvordan norske offentlige sikkerhetsinstitusjoner evner å se at hendelsene er koordinert og at det er en avansert trusselaktør som står bak. Deteksjon handler om etterretningsfunksjonen, men også tverrsektoriell koordinering, samvirke mellom offentlig og privat sektor og internasjonalt samarbeid.

Private virksomheter er sentrale for å detektere sikkerhetstruende hendelser, men de skal ifølge Lov om forebyggende sikkerhet rapporteres videre til myndighetene, og det er i offentlig sektor at det besluttes om dette er en enkeltstående (kriminell) hendelse eller en hybrid trussel, men de private virksomhetenes funksjon vil ikke bli behandlet i detalj. Media spiller også en viktig rolle i krisehåndtering (Olsen et. al. 2008, Boin et. al. 2005). Hvordan 24/7 mediedekning i media påvirker offentlige myndigheters beslutninger er et annet interessant tema som faller utenfor rammene til denne oppgaven.

Datautvelgelse og metode representerer også avgrensninger. Dataene er innhentet gjennom litteraturstudie, og det er ikke benyttet intervjuer. Intervjuer ville ha representert en ytterligere kvalitetssikring av resultatene, men er valgt bort av plass- og tidshensyn. Det ville antakelig vært både tidkrevende og komplisert å finne frem til relevante informanter som kunne belyst den sensitive tematikken i oppgaven. Metoden som er valgt er scenarioutvikling basert på morfologisk analyse. Det er med andre ord ikke en eller flere case-studier av tidligere konflikter som ligger til grunn for analysen, men i stedet et ”syntetisk” empirisk grunnlag basert på et forhåpentligvis transparent utvalg av elementer som til sammen kan sies å gi en uttømmende beskrivelse av hvordan en hybrid trussel kan se ut. Fordelen med denne fremgangsmåten er at den er systematisk og transparent, og dermed etterprøvbar. Samtidig er det viktig å være klar

over at det er en skjønnsmessig vurdering hvilke elementer som velges ut, hvordan de kombineres og hvilke som tas med videre i analysen.

1.4 Kontekst

Dyndal (2010:13) definerer landets strategiske ledelse i krise og krig som det som besluttes i og interaksjonen mellom Utenriksdepartementet (UD), Forsvarsdepartementet (FD) og Justis- og beredskapsdepartementet/JBD. ”Norske offentlige sikkerhetsinstitusjoner" betyr primært etater under FD og JBD: Etterretningstjenesten (E-tjenesten), Nasjonal sikkerhetsmyndighet (NSM) og Politiets sikkerhets tjeneste (PST). Mens selve krisehåndteringen gjerne løses av FD og JBD, vil UD ha en viktig rolle i å trekke de store linjene og sikre at operasjonene underbygger norske strategiske interesser (Dyndal 2010:23). Av hensyn til omfanget vil det legges legge mindre vekt på UDs rolle. En oversikt over norske offentlige sikkerhetsinstitusjoner hentet fra NOU 2016: 19 *Samhandling for sikkerhet* (JBD 2016c) er inkludert i vedlegg A.

I tillegg til departementene og de offentlige sikkerhetsinstitusjonene, danner også prinsippene nasjonalt sikkerhets- og beredskapsarbeid et rammeverk for analysen. *Ansvarsprinsippet* innebærer at den organisasjonen som har ansvar for et område til daglig, også har ansvaret for å forberede beredskap og håndtering av ekstraordinære hendelser på området. *Likhetsprinsippet* betyr at den organiseringen som brukes i normalsituasjoner i størst mulig grad skal videreføres i en krisesituasjon. I følge *nærhetsprinsippet* skal en krise håndteres på lavest mulige organisasjonsnivå. Samvirkeprinsippet betyr at involverte aktører på alle nivåer har selvstendig ansvar for å sikre samvirket med andre aktører i arbeidet med forebygging, beredskap og krisehåndtering (JBD 2016:182). Nærhetsprinsippet gjelder imidlertid ikke ved sikkerhetspolitiske kriser (DSB 2015:11).

Det nasjonale beredskapsapparatet i Norge er inndelt i tre nivåer: strategisk, operasjonelt og taktisk (JBD 2016:183). Selv om taktisk og operasjonelt nivå vil være sentrale i deteksjon og håndtering av hendelser av den typen som beskrives i scenarioene, vil fokus primært være på det sentrale apparatet, der den strategiske situasjonsforståelsen vil bli etablert i en krisesituasjon.

Strategisk nivå består av Regjeringen, Kriserådet og departementene. Hver enkelt statsråd er ansvarlig for sin sektor i henhold til ansvarsprinsippet. I en krisesituasjon vil det utpekes et lederdepartement som har ansvar for koordinering på departementsnivå. JBD ivaretar rollen som

lederdepartement i sivile nasjonale kriser med mindre annet er bestemt (JBD 2016:183, DSB 2015:12).

Krisekoordinering skjer i Kriserådet. Rådet består av ledende embedsmenn ved Statsministerens kontor (SMK), UD, FD, JBD og Helse- og omsorgsdepartementet (HoD). Rådet møtes ikke bare ved kriser, men har en fast møtestruktur. Deltagelsen kan ved behov utvides med representanter fra andre departementer, underliggende virksomheter og særskilte kompetansemiljøer (JBD 2016:183, DSB 2015:12).

Lederdepartementet og Kriserådet støttes av Krisestøtteenheten, KSE (JBD 2016:184). KSEs funksjon er å bidra til økt kapasitet for krisehåndtering i departementene, og skal ikke overta ansvar eller oppgaver som hører til departementenes linjeansvar (DSB 2015:13). Nasjonalt sivilt situasjonssenter er plassert i KSEs lokaler, men er i det daglige underlagt JBD. Situasjonssenteret er døgnbemannet og har ansvar for varsling og analyse av situasjonsbildet i kriser. Dermed vil den strategiske situasjonsforståelsen bli forvaltet her, basert primært på rapportering fra andre virksomheter i justissektoren - PST, POD, DSB, NSM og HRS. Situasjonssenteret mottar også rapporter fra andre sektorer som sammenstilles og analyseres, og samarbeider med UDs operative senter og Forsvarsdepartementet/Forsvarsstabens situasjonssenter SITSEN (*ibid.*:14).

Regjeringskollegiet behandler spørsmål knyttet til samfunnssikkerhet og beredskap i ulike sammenhenger, primært i plenum (SMK 2017a:9). Saker som krever begrenset spredning av informasjon, spesielt knyttet til forsvar, sikkerhetspolitikk eller beredskap, kan imidlertid etter statsministerens ønske behandles i Regjeringens sikkerhetsutvalg (RSU). Faste medlemmer i RSU er statsministeren, justis- og beredskapsministeren, forsvarsministeren, finansministeren og utenriksministeren. Andre statsråder inkluderes ved behov (JBD 2016:183). De ulike tjenestene på sivil og militær side møter også i RSU. Det er etablert et fast sekretariat bestående av representanter for SMK, UD, JBD og FD. SMK presiserer at opprettelsen av et sekretariat ikke endrer rolle- og ansvarsfordelingen mellom SMK og departementer, og at operativt sikkerhetsarbeid ikke vil utføres av RSU-sekretariatet (SMK 2017a:10, SMK 2015).

I FD er Avdeling for sikkerhetspolitikk og operasjoner (FD II), ved seksjon for Nasjonal sikkerhetspolitikk, krisehåndtering og beredskap (FD II-4) ansvarlig for å organisere, lede og koordinere krise- og episodehåndtering (FD u.å.). FD II-4 skal ved sikkerhetspolitiske kriser eller nasjonale kriser der Forsvaret støtter sivil sektor etablere en analyse- og koordineringsgruppe som utgjør FDs krisestab. I Forsvarets situasjonssenter, SITSEN, vil operasjonsavdelingen møtes for å ivareta fagmilitære spørsmål (Flakstad 2010:317-318). Den sikkerhetspolitiske analyse- og koordineringsgruppen og den militære koordineringsgruppen i SITSEN skal jobbe integrert og levere helhetlige råd til departementets ledelse (*ibid.*:325). Organiseringen av strategisk krisehåndtering i forsvarssektoren er lagt opp til å være fleksibel og legge til rette for tilpasning til kriser av ulik karakter, enten de er av sivil (med Forsvaret som støtte til lederdepartementet og sivilsamfunnet) eller av sikkerhetspolitisk art (*ibid.*:320). Deteksjon, varsling og håndtering av kriser på strategisk nivå understøttes av en rekke aktører som jobber døgnkontinuerlig. Ved siden av Nasjonalt sivilt situasjonssenter, UDs operasjonssenter og Forsvarets SITSEN, jobber også en rekke virksomheter på operativt nivå 24/7, som Forsvarets operative hovedkvarter (FOH), Politidirektoratet (POD), PST og NSM/NorCERT (JBD 2016:134, Forsvaret 2017).

NSM er landets forebyggende sikkerhetstjeneste og har sitt mandat gjennom Sikkerhetsloven. NSM skal koordinere forebyggende sikkerhetstiltak, så som fysisk sikring, personellsikkerhet og informasjonssikkerhet og dessuten føre tilsyn med sikkerhetstilstanden i virksomheter som er underlagt sikkerhetsloven. NSM drifter NorCERT, den nasjonale enheten for nettverksovervåking og VDI, Varslingssystem for digital infrastruktur (NSM 2014a/b, Lysne II 2016:23).

PSTs oppgaver er beskrevet i Politiloven og omfatter å forebygge, motvirke og etterforske lovbrudd mot statens sikkerhet og selvstendighet, ulovlig etterretningsvirksomhet, ulovlig teknologioverføring, spredning av masseødeleggelsesvåpen, samt sabotasje og politisk motivert vold med utgangspunkt i Straffeloven, Lov om forsvarshemmeligheter og Sikkerhetsloven. PSTs oppgaver kan sammenfattes som etterretnings-, etterforsknings- og sikkerhetsvirksomhet, herunder rådgivning og livvakttjeneste (Justis- og beredskapsdepartementet 2012:12, PST u.å.).

I følge Lov om Etterretningstjenesten (1998) skal tjenesten ”innhente, bearbeide og analysere informasjon som angår norske interesser sett i forhold til fremmede stater, organisasjoner eller individer, og på denne bakgrunn utarbeide trusselanalyser og etterretningsvurderinger, i den utstrekning det kan bidra til å sikre viktige nasjonale interesser”. E-tjenesten skal produsere beslutningsstøtte for myndighetene, ikke drive straffeforfølgning, og skal heller ikke drive overvåking av nordmenn i Norge (Lysne II 2016:5).

Direktoratet for samfunnssikkerhet og beredskap (DSB) produserer oversikter over risiko og sårbarhet i samfunnet. DSB vurderer risiko i et *all hazards*-perspektiv knyttet til katastrofale hendelser som kan ramme samfunnet: naturhendelser, ulykker og tilsiktede handlinger. Analysene fra DSB har et lengre tidsperspektiv enn de årlige vurderingene fra E-tjenesten, NSM og PST (PST 2017).

NSM, PST og E-tjenesten samarbeider og utveksler informasjon på ulike nivåer og fagområder, noe som er viktig for å håndtere et komplekst og dynamisk trusselbilde (PST u.å.).

På ledelsesnivå møtes representanter for FD, JBD og UD og sjefene for de tre tjenestene i Koordinerings- og rådgivingsutvalget for etterretnings-, overvåkings- og sikkerhetstjenestene (KRU). Ved siden av å koordinere tjenestenes oppgaver, prioriteringer og mål, skal KRU analysere og utrede felles problemstillinger knyttet til trusselbildet (JBD 2002).

Felles kontraterrorsenter (FKTS) er en samarbeidsmekanisme mellom PST og E-tjenesten på kontraterrorområdet. FKTS skal blant annet ivareta informasjonsdeling mellom tjenestene og sammenstille analyser og trusselvurderinger. Senteret driver ikke egeninnhenting, og medfører ingen endringer i de to tjenestenes mandat (Lysne II 2016:22).

Felles cyberkoordineringssenter (FCKS) er en samarbeidsmekanisme mellom NSM, E-tjenesten, PST og Kripos. Formålet med senteret er å styrke nasjonal evne til effektivt forsvar mot og håndtering av alvorlige hendelser i det digitale rom. FCKS skal koordinere hendelseshåndtering, lage innledende vurderinger av hendelser og gi anbefaling til virksomhetene som har ansvar for den videre håndteringen (NSM 2017:37, 49).

2. Arbeidsform og metoder

Dette kapittelet gjør rede for forskningsdesign, arbeidsprosessen som er fulgt i utarbeidelsen av oppgaven og hvilke metoder (med tilhørende styrker og svakheter) som er valgt for å besvare problemstillingen.

2.1 Forskningsdesign

Forskningsdesignet er forskerens interne arbeidsdokument som skal utarbeides før arbeidet tar til. Hensikten er å ha en rettesnor for arbeidet, og sikre at man ikke mister kontroll over prosessen. Designet skal inkludere alle beslutninger som gjøres i forskningsarbeidet, og eksponere disse for kritisk evaluering fra andre (Blaikie 2010:12). Det er imidlertid mulig å gjøre endringer på designet etter hvert som arbeidet skrider frem, og justeringer har vært nødvendige i arbeidet med denne oppgaven.

Basert på egen arbeidserfaring fra Forsvaret kombinert med teoretisk påfyll fra masterstudiet ved UiS, har forfatteren en interesse for hvordan samfunnet kan bli bedre i stand til å håndtere tilsiktede trusler. Det finnes mye forskning som ser på risikohåndtering i forbindelse med terrorisme, kriminalitet og cyberangrep. På disse områdene er tverrsektorielt samarbeid sentralt, og samtidig komplisert. Dette gjør samfunnet sårbart. En trusselaktør som benytter hybride metoder utnytter denne sårbarheten gjennom å handle fordekt i ulike domener på en måte som gjør samarbeid og påfølgende beslutningstaking komplisert for forsvareren.

Det finnes mye litteratur som fokuserer på å definere hybride trusler og om begrepet egentlig inneholder noe nytt. Det er også skrevet en god del om hvordan samfunnet skal forsvare seg mot denne typen trusler. Denne delen av litteraturen fokuserer primært på hvordan *konsekvensene* av et angrep kan reduseres, spesielt gjennom oppbygging av resiliens. Dimensjonen *sannsynlighetsreduksjon*, herunder deteksjon av truslene, representerer derimot et visst hull i forskningen. Dette kan skyldes at denne tematikken i stor grad hører inn under sikkerhets- og etterretningstjenesters mandater, og dermed kommer i berøring med gradert materiale. I denne oppgaven har er det kun benyttet allment tilgjengelige og ugraderte kilder.

Forsvarets forskningsinstitutt sitt BAS 8-prosjekt (Sivil-militær krisehåndtering og beredskap) inkluderer blant annet problemkomplekset «Totalforsvaret i en hybridkrigføringskontekst», der et hovedspørsmål er hvorvidt hybride trusler representerer noe nytt for norsk samfunns- og statssikkerhet. Det finnes en rekke mulige tilnærminger: Ansvarsforhold, beredskapsplanlegging, hvordan man skal respondere. Denne oppgaven handler om hvordan man evner å se at hendelser er koordinert, det vil si hvordan norske sikkerhetsinstitusjoner kan detektere at de står overfor en hybrid trussel, og ikke en rekke isolerte hendelser.

Jacobsen (2015:63) skiller problemstillinger i om de på den ene siden er deskriptive eller forklarende/kausale og på den andre siden er utforskende/eksplorerende eller testende. Min valgte problemstilling er forklarende/kausal på den måten at den søker å beskrive hvilken effekt en potensiell ytre påvirkning (en hybrid trussel) vil ha på et sosioteknisk system (norske sikkerhetsinstitusjoner). Undersøkelsen stanser ikke ved å kun beskrive de to fenomenene, formålet er å beskrive sammenhengene mellom dem, hvilken effekt ytre påvirkning har på systemet. Problemstillingen er videre eksplorerende i den forstand at den skal utdype et fenomen der kunnskapen er begrenset. Samtidig er den testende, for å forsøke å finne rekkevidden eller omfanget av fenomenet *hybrid trussel fra statlig aktør mot Norge*.

Blaikie (2010:59) definerer tre hovedkategorier av forskningsspørsmål: «hva», «hvorfor» og «hvordan». De ulike kategoriene har betydning for selve formålet med forskningen. «Hva» handler om beskrivelser, «hvorfor» søker etter forklaringer, og «hvordan» har som hensikt å lede til endringer, med praktiske resultater og intervensjon. Spørsmålstillingen om hvordan man kan se at hendelser er koordinert, leder dermed implisitt til at resultatet av forskningen kan bestå av anbefalinger om hvordan praksis kan endres.

Forskningsspørsmålene leder videre til ulike strategier for å finne svarene. Blaikie (2010) angir følgende fire forskningsstrategier: induktiv, deduktiv, retroduktiv og abduktiv. Det kan være nødvendig å bruke en kombinasjon av disse. Oppgaven benytter en deduktiv tilnærming for å beskrive fenomenet hybride trusler (et «hva»-spørsmål), gjennom datainnsamling (litteraturstudie) og generaliseringer om karakteristikkene til fenomenet. I arbeidet med å teste scenarioer opp mot norske sikkerhetsinstitusjoner (et «hvordan»-spørsmål) er en abduktiv

tilnærming mer relevant. Denne tar utgangspunkt i observasjoner (empiri) og har som mål å beskrive og forstå sosiale prosesser, gjennom å utforske sosiale aktørers meninger, fortolkninger, motiver og forklaringer (Blaikie, 2010). En abduktiv forskningsstrategi er en blanding av induksjon og deduksjon, og har preg av å være en kontinuerlig problemløsende prosess, der man søker etter sannsynlige beskrivelser og forklaringer (Jacobsen 2015:35).

Forskningsparadigmet som er benyttet er basert på en filosofisk tilnærming inspirert av Karl Popper, som forkaster både positivismens antakelse om en objektiv verden styrt av lovmessighet, og den fortolkningsbaserte oppfattelsen om at alt er unikt (Jacobsen 2015:32). Popper mener at det ikke er mulig å uttale seg sikkert om årsaksforhold innen samfunnsvitenskap. Men det finnes like vel hendelser som gjentar seg med en viss grad av regelmessighet i sosiale systemer. Han benytter en form for sannsynlighet (*propensity*), som gjør det mulig å komme frem til forklarende utsagn av typen «hvis A skjer, øker sannsynligheten for at B vil inntreffe» (Thorsvik 2000 i Jacobsen 2015:32). De forventede resultatene av analysen er derfor åpenbart ikke allmenngyldige sannheter, men de vil forhåpentligvis kunne illustrere med en grad av sannsynlighet hvordan norske myndigheter ville håndtert en situasjon der de stilles overfor en hybrid trussel og peke på noen svakheter og mangler i systemet. Et sosial-konstruktivistisk perspektiv tilsier at angrep er reelle, men at betydningen de tilskrives og de politiske konsekvensene de får er konstruert (Jore 2012:vii). Det er også en politisk handling å definere et tema som en sikkerhetstrussel, å "sikkerhetisere" det, med de implikasjonene dette får i form av ekstraordinære tiltak utenfor ordinære politiske prosedyrer (Buzan et. al. 1998:24). Det epistemologiske utgangspunktet for undersøkelsen er dermed at det finnes enkelte trekk ved virkeligheten som det er bredere enighet om enn om andre. Forskningen består dermed i å samle inn empiri, informasjon fra virkeligheten, som vil være mer eller mindre objektiv eller konstruert, og fortolke denne (Jacobsen 2015 33-34).

2.2 Metode

Det følgende avsnittet gjør rede for metodene som er benyttet for datainnsamling: litteraturstudien og den morfologiske analysen som ligger til grunn for scenarioutvikling. Jacobsen (2015:35) skiller mellom åpen og lukket datainnsamling, det vil si i hvilken grad forskeren legger begrensninger på dataene som skal hentes inn i forkant av undersøkelsen. I en abduktiv tilnærming vil valget mellom åpen og lukket datainnsamling avhenge av hvor forskeren

befinner seg i kunnskapsutviklingen. En åpen eller eksplorativ tilnærming er fornuftig for å utvikle en dypere forståelse for fenomenet på et tidlig stadium. I denne oppgaven representerer litteraturstudien en slik åpen undersøkelse. Med en grundigere forståelse for fenomenet har det deretter blitt mulig å gjennomføre en mer stringent og lukket morfologisk analyse av hvordan en hybrid trussel mot Norge kan se ut, der fenomenet brytes ned i sine enkeltbestanddeler og testes for hvilke kombinasjoner som er mulige.

2.2.1 Litteraturstudie

En hovedutfordring i arbeidet har vært å skape klarhet i hybridbegrepet, som er både diffust og omstridt. Dette er forsøkt løst gjennom en gjennomgang av betydelige mengder primær- og sekundærkilder for å skape en ramme og for å definere problemet ytterligere. Det har vært viktig å ha en kritisk holdning til hvilke kilder som inkluderes. Tematikken er politisk betent, ved at man fra vestlig hold mener at Russland bedriver hybridkrig i Ukraina og står bak cyberangrep og påvirkningsoperasjoner mot europeiske land. Russiske kilder bruker hybridbegrepet for å beskrive det de oppfatter som forsøk på undergraving av deres regimestabilitet. Noen primærkilder fra russisk militært hold er derfor benyttet, først og fremst Gerasimov (2013, 2017), Chekinov og Bogdanov (2010) og Myasnikov (2005). Svechin (1926) og Messner (2005) er relevante for forståelsen av hybridkrig i en russisk historisk kontekst, og er behandlet i vedlegg B.

Primærkildene består ellers av offentlige policy-dokumenter (norske og utenlandske, spesielt fra NATO og EU-hold) som beskriver eksisterende og planlagte tiltak for å møte trusselen og håndtere risikoen. Norske NOU-er og stortingsproposisjoner har en sentral plass, siden det er det norske ”sikkerhetssystemet” som skal studeres. De viktigste er Meld. St. 10 *Risiko i et trygt samfunn* (JBD 2016), Prop. 153 L *Lov om nasjonal sikkerhet (sikkerhetsloven)* (FD 2017a), *Støtte og samarbeid* (FD 2015a). Ugraderte trussel- og risikovurderinger fra de norske etterretnings- og sikkerhetstjenestene er benyttet for å gi et bilde av norske myndigheters risikoforståelse og hvordan de kommuniserer denne til befolkningen. Disse kildene er supplert med tilsvarende vurderinger fra baltiske land, der presset fra Russland oppleves som spesielt stort.

Nyhetsreportasjer er også til en viss grad benyttet for å gi ytterligere kontekst til utarbeidelsen av scenarioer. Der en nyhetskilde fra en side i en konflikt er benyttet, er dette angitt slik at det fremkommer at det for eksempel er ukrainske kilder som rapporterer om russiske handlinger.

Sekundærkilder i denne oppgaven består for det første av teoretiske perspektiver og forskning på fenomenet hybride trusler. Forskningslitteraturen er valgt ut for å finne relevante teoretiske perspektiver som kan bidra til å besvare problemstillingen og for å beskrive så mange aspekter av trusselen som mulig, og dermed bidra til at scenarioene, det empiriske grunnlaget, blir relevant for den avsluttende drøftingen.

Teorigjennomgangen består av litteratur fra henholdsvis risiko- og etterretningsstudier. Risikofaget inneholder en rekke teoretiske perspektiver hentet fra studier av utilsiktede hendelser (safety) som kan bidra til å belyse problemstillinger knyttet til tilsiktede handlinger (security). Etterretningsstudier er et felt som utviklet seg med åpenheten rundt nasjonale sikkerhetsspørsmål som fulgte etter den Kalde krigen, og i enda større grad etter 2001, da med et særlig fokus på etterretningsfadeser som terrorangrepene i USA og Irak-krigen. Etterretningsstudier er imidlertid i stor grad er basert på empiriske studier, og har i mindre grad vært opptatt av teoretisering og konseptutvikling (Gill 2010). Her kan perspektiver fra risikofaget bidra, noe som kan være verd en egen studie i seg selv. Ordlisten fra Society for Risk Assessment (SRA 2015) bidrar til enhetlig begrepsbruk. Risikobegrepets ulike aspekter dekkes av Busmundrud et. al. (2015), Aven (2007, 2013) og Aven og Krohn (2014). Mazarr (2016) diskuterer bruken av risikostyring innen sikkerhetspolitikk. Vandepeer (2011) presenterer et utvidet trusselbegrep, mens Foley (2009, 2013) har en relevant modell for trusselpersepsjon. Avsnittet om krisehåndtering er i stor grad basert på Olsen et. al. (2008), Boin et. al. (2005), Kruke (2005) og McCarthy (1998). Klassikere innen etterretningsstudier er representert ved Betts et. al (2005), Herman (1997), Wohlstetter (1962) og Grabo (2002), mens Dunn Cavelty og Mauer (2009) og Rathmell (2002) bringer inn nye perspektiver fra risikostudier. Kilder til systemfeil dekkes av blant annet Reason (1997), Turner (1976) og Turner og Pidgeon (1997), mens studiene til Sagan (1993), Westrum og Adamski (1993) og Rasmussen (1997) ser på måter slike feil kan motvirkes. De viktigste kildene for gjennomgangen av hybride trusler er Hoffman (2007, 2017), Reichborn Kjennerud og Cullen (2016), artikkelsamlingen fra (Renz og Smith 2016), Galeotti (2016a, b), Cederberg og Eronen

2015, Kofman og Rojanski (2015), Mazarr (2015), Giegerich (2016), Thiele (2016), Chivvis (2017), og Murray og Mansoor (2012) som illustrerer hybridkrig i et historisk perspektiv. Artiklene om hybride trusler omfatter både anglo-amerikanske og europeiske forfattere.

2.2.2 Morfologisk analyse og scenarier

Eksempler på konflikter der hybride trusler forekommer finnes både i nær og fjernere historie. Gjennom å studere historiske eksempler kan man lære mye om hvordan en trussel kan settes sammen. Men i erkjennelse av at enhver kampanje vil være unik og tilpasset sårbarhetene i det systemet eller staten som angripes, er det valgt en scenario-tilnærming snarere enn rene case-studier av tidligere hybride kampanjer, for bedre å kunne beskrive hvordan slike trusler rettet mot Norge vil kunne se ut. Scenarioene er resultat av en morfologisk analyse basert på metoden *General Morphological Analysis* (GMA). Den morfologiske analysen er basert på litteratur om hybride trusler, i stor grad knyttet til Russland, men også Kina for å få et bredere grunnlag og ikke ensidig låse analysen til Russland/Ukraina-tematikken. Med grunnlag i analysen etableres en typologi over hybride trusler, som igjen danner grunnlag for scenarioer.

I følge Meyer (2009:10) skal en typologi tilfredsstille en rekke krav. For å svare på problemstillingen må den være praktisk brukbar, det vil si at den må inneholde informasjon som gjør det mulig å lage scenarioer som kan benyttes til å illustrere utfordringen rundt deteksjon av hybride trusler for norske sikkerhetsinstitusjoner. Scenarioene skal være realistiske i den forstand at de inkluderer hendelser som *kan* inntreffe, selv om sannsynligheten for dette er lav. Typologien må være forståelig for leseren og godt begrunnet. Den bør være dekkende eller uttømmende, det vil si at den må inneholde alle relevante aspekter ved hybride trusler. Den bør også være gjensidig utelukkende på den måten at det blir rimelig enkelt å plassere de ulike enhetene i sine kategorier. På slutten av kapittel 4 vurderes det i hvilken grad typologien klarer å tilfredsstille disse kravene.

Scenario er et velegnet beslutningsverktøy for å håndtere usikkerhet. Det eksterne miljøet rundt en organisasjon preges av uventede endringer, og det kan være utfordrende å få øye på tvetydige trender. Scenarioanalyse har ikke som formål å forutsi fremtiden, men stiller opp ulike bilder på hvordan det eksterne miljøet kan utvikle seg, og dermed kan man få frem kritiske usikkerheter

som vil virke inn på strategiske valg (Postma og Liebl 2005:162). Scenarioanalyse er imidlertid ikke en entydig metode. Gjennom de siste 30 årene har det blitt utviklet en rekke teknikker og metoder som til tider er selvmotsigende (Bradfield et. al. 2005:795).

GMA er en metode for å strukturere og undersøke relasjoner i flerdimensjonale, ikke-kvantifiserbare problemkomplekser (Ritchey 2006:1). Modellen er velegnet til å utvikle scenarioer og strategiske alternativer. Den har blant annet blitt benyttet ved FFI for å etablere scenarioer i forbindelse med Forsvarsstudie 2007 (Johansen 2006), for å etablere en typologi over uønskede hendelser som kan true nasjonal sikkerhet (Meyer 2009) og for å analysere fremtidige operasjonstyper det norske forsvaret kan bli involvert i fremtiden (Diesen 2016). Martins et. al. (2012) har benyttet metoden for å etablere en modell for informasjonssikkerhet for militære organisasjoner. GMA er en egnet metode for å modellere og analysere *wicked problems*, altså komplekse samfunnsmessige og organisasjonsmessige planleggingsutfordringer som mangler en klar formulering, er umulige å si når er "løst", henger sammen med andre problemkomplekser og er i stadig endring (Ritchey 2013). Kosow og Gaßner (2008:18) nevner fire bruksområder for scenarioer: utforskning, kommunikasjon, mål-setting og beslutningstagning/strategiutforming. Dunn Cavelty et.al (2011:4) skiller mellom to bruksområder: *foresight* og risikovurdering. Scenarioene i denne oppgaven utarbeides primært i et *foresight*-perspektiv.

Metoden er i tillegg velegnet for å sette framtidsscenarioer basert på faktorer som er utenfor ens kontroll (det kontekstuelle miljøet) opp mot løsningsstrategier, eller det interne miljøet som man har kontroll over (Ritchey 2006:7). Det blir for omfattende i denne oppgaven å gjøre en analyse der man setter et scenario-felt opp mot et strategi-felt. Derfor vil scenarioene (hybride trusler) bli vurdert opp mot strategier (i denne oppgaven forstått som kapabiliteter og samvirke i norsk kontekst) kun gjennom den avsluttende drøftingen i kapittel 6. Dette kan være en svakhet ved analysen.

Fremgangsmåten i GMA er i følge Johansen (2006:10):

1. formuler en presis problemstilling,
2. identifiser og analyser alle dimensjoner eller parametere som er relevante for problemet,

3. identifiser verdier for hver parameter i en morfologisk boks,
4. eliminer verdier som ikke kan opptre samtidig (er inkonsistente)
5. velg ut de optimale løsningene

Arbeidet med å definere verdier og parametere og sette dem i inn i en morfologisk matrise som gir et håndterbart resultat er tidkrevende, og det viste seg nødvendig å forkaste mange versjoner av analysen. Den fullstendige konsistensmatrisen finnes i vedlegg B.

Den største svakheten ved datautvalg og metode er trolig at det ikke har vært tid til å gjennomføre intervjuer med personer som kunne bidratt med ekspertinnspill til den morfologiske analysen. Ideelt sett skal analysearbeidet foregå i workshops med ulike fageksperter til stede (Ritchey 2011:89.2006:1). Det har derfor vært nødvendig med en rekke skjønnsmessige vurderinger for å finne relevant litteratur og gjennomføre den morfologiske analysen på en slik måte at den gir et resultat som kan brukes til å utvikle relevante scenarier.

3. Teoretiske perspektiv

Hensikten med gjennomgangen av teoretiske perspektiver er å belyse problemstillingen og forskningsspørsmålene ytterligere. Kapittelet er delt i to. Den første delen omhandler sikringstiltak, og ser på risikostyring, krisehåndtering og teori knyttet til deteksjon av farer. Perspektivene er hentet fra både risiko- og etterretningsstudier. Teorien fra risikofaget har det til felles at den omhandler hvordan svake signaler kan detekteres i organisasjoner, og hvordan en kommende krise kan gjenkjennes. Teoriene er utviklet primært fra et safety-perspektiv og med bakgrunn i studier av organisasjoner, men i denne oppgaven vil de bli forsøkt anvendt på samfunnsnivå. De teoretiske perspektivene fra etterretningsstudier, et mer underteoretisert fagfelt, omhandler tematikk som etterretningsfadeser og indikasjon og varsling, som er metodikk utviklet for deteksjon av trusler. Den andre delen av teorikapittelet handler om trusselen, altså hybridbegrepets innhold og relasjon til beslektede begreper. En historisk fremstilling av begrepet finnes også i vedlegg A. Til sammen skal de to delene lede frem til en modell eller noen prinsipper for hvordan hybride trusler kan detekteres, og vil således være relevant for den avsluttende drøftingen av scenarioer.

3.1 Sikringstiltak

3.1.1 Risiko og trussel, sikkerhet og usikkerhet

Sikkerhet, usikkerhet, trussel og risiko er sentrale begreper for den videre drøftingen. Det er samtidig begreper som har en rekke ulike definisjoner og tolkninger. Risikobegrepet og risikoanalyser er primært knyttet til myndighetenes arbeid med forebyggende sikkerhet og beredskapsplanlegging samt til beslutningstagernes vurdering av hvilken respons en trussel skal møtes med. Trussel er en kilde til risiko, og deteksjon handler om å avdekke og vurdere trusselen, slik at trusselvurderingen kan inngå i det videre arbeidet med å håndtere risiko. Aradau et.al. (2008:148) understreker at trusselbaserte tolkninger av sikkerhet baserer seg på etterretning med det formål å eliminere farer, mens et risikobasert syn på sikkerhet derimot handler om å finne måter å leve med risiko og bygge beredskap. Trusselvurderinger er imidlertid viktig grunnlagsinformasjon for risikoanalyser (*ibid.*). I en situasjon der man kun har en tredjedel av midlene for de mest åpenbare sikkerhetstiltakene er etterretningsanalyser nødvendige for å prioritere størrelsen på investeringene og hvilke områder som er mest sårbare (Perrow 2006).

Sikkerhet: Safety og security

Sikkerhet (security) kan defineres som fravær av uakseptabel risiko fra tilsiktede handlinger fra intelligente trusselaktører. Sikkerhet er i dette perspektivet det motsatte av risiko: sikkerhetsnivået er knyttet til risikonivået, slik at et høyt sikkerhetsnivå betyr lav risiko (SRA 2015:10). Buzan et. al. (1998:5) peker på at sikkerhet er mer enn en trussel eller et problem. Et sikkerhetsspørsmål defineres som en trussel mot et referanseobjekt av en aktør med myndighet til å godkjenne ekstraordinære tiltak som går ut over vanlige regler. Sikkerhet betyr ulike ting i ulike kontekster. Safety er knyttet til (intern) risiko som en organisasjon velger å utsette seg for gjennom sin ordinære virksomhet, mens security er knyttet til (ekstern) risiko som organisasjonen blir utsatt for (Jore og Egeli 2015:807). Safety handler om beskyttelse mot farer, security er beskyttelse mot trusler (Statoil ASA 2013:75). Over tid har safety og security utviklet seg som to separate fagområder, hver med sine egne verktøy og metodikker. Det finnes imidlertid stort potensiale for at verktøy og metodikk utviklet i den ene disiplinen kan benyttes i

den andre (Pièrre-Cambacédès og Bouissou 2013:111)[2]. Både safety og security har imidlertid det til felles at det handler om beskyttelse mot risiko, mens det er opphavet til risikoene, risikokildene, som er forskjellig.

Usikkerhet: Epistemisk og ontologisk

Usikkerhet er mangelfull eller ufullstendig informasjon eller kunnskap om en hypotese, en mengde eller om en hendelse vil inntreffe (SRA 2015:4-5). Det finnes to hovedtyper av usikkerhet – epistemisk og ontologisk. I en tilstand av epistemisk usikkerhet er ikke problemet at fremtiden er teoretisk umulig å kjenne. Problemet er at beslutningstagerne ikke kan få nok informasjon til å forstå hva som vil skje (Mazarr 2016:59). Ontologisk usikkerhet er mer grunnleggende. Den handler om at fremtiden ennå ikke eksisterer, og at den skapes av en mengde fenomen som interagerer med hverandre. Fremtiden skapes kontinuerlig, og den "finnes ikke" i tilgjengelig informasjon, uansett hvor mye vi måtte samle inn (*ibid.*). Usikkerheten knyttet til deteksjon av hvorvidt ulike hendelser kan defineres som en hybrid trussel handler om i hvilken grad hendelsene er koordinert, og om det dermed ligger en politisk intensjon bak. Denne usikkerheten reduseres dermed gjennom å forsøke å avdekke hvilke aktører som står bak og hva deres intensjon er. Dette er informasjon som eksisterer, men som kan være svært vanskelig å finne, siden staters strategiske målsetninger vil være beskyttet og hemmeligholdt. Etterretning er et viktig verktøy for å redusere usikkerheten knyttet til internasjonale relasjoner generelt, og hybride trusler spesielt (Fägersten 2017:1).

Risiko

Risiko kan på et høyoppløselig nivå defineres som muligheten for en uønsket hendelse eller potensialet for at en hendelse vil utløse uønskede og negative konsekvenser (SRA 2015:3). Risiko er fremtidsrettet og blir virkelige dersom de manifesterer seg. Risiko er det som kan skje, snarere enn det som foregår, og scenarioer er et nyttig virkemiddel for å *snakke* om risiko (Dunn

[2] IKT-området kan illustrere dette. Her stod safety engineering sentralt på et tidligere utviklingsstadium. Dette var relativt uproblematisk så lenge kritiske systemer var proprietære og stand-alone. Etter hvert som datasystemer har blitt distribuert og koblet i nettverk, inkludert kritiske systemer, har security-risikoer som databeskyttelse, privacy, virus, denial of service attacks osv. fått økende oppmerksomhet (Schoitsch 2005).

Cavelty et. al. 2011:6, 8). Risiko er ikke bare negativt. Det å ta risiko kan gi økonomisk gevinst, og gjennom å søke risiko og mestre farer kan mennesker også oppnå økt livskvalitet (Aven 2007:37-38). Risiko skal dermed ikke ensidig fjernes, men styres (*ibid.*). Det er imidlertid de negative konsekvensene som er tema i denne oppgaven. Det tradisjonelle synet er at risiko er en kombinasjon mellom sannsynlighet og konsekvens. Man skiller mellom to typer sannsynlighet: *relativ frekvenstolket sannsynlighet* som beskriver variasjon og *subjektiv/kunnskapsbetinget sannsynlighet* som beskriver usikkerhet (eller mangel på kunnskap). Men sannsynlighet er bare ett av flere verktøy for å beskrive usikkerhet. Det har de siste årene blitt lansert ulike perspektiver på risiko som erstatter sannsynlighet med usikkerhet. (Aven og Krohn 2014:1).

I norsk sammenheng har det blitt utviklet to standarder for risikovurderinger: NS 5814:2008, som definerer risiko som "uttrykk for kombinasjonen av *sannsynlighet* for og *konsekvensene* av en uønsket hendelse". Den andre standarden, NS 5832:2014, er utarbeidet spesifikt for beskyttelse mot uønskede tilsiktede handlinger, og definerer sikringsrisiko som "uttrykk for forholdet mellom *trusselen* mot en gitt *verdi* og denne verdiens *sårbarhet* overfor den spesifiserte trusselen". Denne tilnærmingen er også kjent som trefaktormodellen, og ligger til grunn for mye av norske myndigheters arbeid med tilsiktede trusler (Busmundrud et. al. 2015:9, FD 2016c:41, FD 2017a:15). Trefaktormodellen har imidlertid møtt motbør. Hovedskillet mellom de to tilnærmingene er vekten som legges på sannsynlighetsvurderinger. NS 5832:2014 refererer ikke eksplisitt til sannsynlighetsbegrepet, siden det er vanskelig å vurdere sannsynlighet for tilsiktede handlinger som inntrer uhyre sjelden. Samtidig bruker standarden sannsynlighet indirekte ved at man er nødt til å velge ut noen scenarioer som grunnlag for analysen (Busmundrud et. al. 2015:16). Sannsynligheten for tilsiktede uønskede handlinger og den tilknyttede usikkerheten kan ikke ignoreres. Sannsynligheten bør imidlertid tolkes som anbefalt av blant annet Aven (2013:143) og Aven og Krohn (2014:8) – ikke matematisk og frekvensbasert, men subjektivt og kunnskapsbasert - og kunnskapsgrunnlaget som ligger til grunn for vurderingen må presenteres for beslutningstagerne slik at gode valg kan tas om prioritering av ressursene (Amundrud et. al. 2017:292).

Jore (2012:3) konstaterer at det har vært svært lite debatt om hvorvidt antiterror-tiltak i Norge har en risikoreduserende effekt. Man har i stedet fokusert på samfunnets trusselpersepsjon. Knutsen (2010:370) peker på at endringen av Forsvarets fra invasjonsforsvar under den kalde krigen til å delta i *out-og-area*-operasjoner i Afghanistan og Irak reflekterer overgangen fra et nasjons- og trusselfokusert til et internasjonalt og risikofokusert sikkerhetsbegrep. Fra å være dimensjonert for å håndtere en kjent, om enn monumental, *trussel* om invasjon fra Sovjetunionen, ble oppgavene i større grad å bidra til håndtering av mindre håndgripelige *risikoer* som internasjonal terrorisme langt borte fra Norge. Afghanistan-utvalget (FD 2016d:58) peker på at det viktigste målet med norsk deltagelse i Afghanistan var å støtte NATO og særlig USA, og dermed kan den norske innsatsen også tolkes som et tiltak for å redusere risikoen for at Norge blir stående uten alliert hjelp i en krevende sikkerhetspolitisk situasjon nasjonalt.

Trussel

Trussel defineres som en risikokilde, vanligvis i forhold til tilsiktede handlinger. En trussel i forhold til et angrep er en uttalt eller utledet intensjon om å utføre et angrep i den hensikt å påføre skade, frykt, smerte eller ulykke (SRA 2015:11)[3]. En trussel er dermed et element i risiko. Trussel vurderes vanligvis som en funksjon av intensjon om og kapabilitet til å utføre en tilsiktet uønsket handling. Denne tradisjonelle oppfatningen av trussel kritiseres blant annet av Vandepeer (2011), som sporer intensjon/kapabilitet-tilnærmingen tilbake til Singer (1958), som var den første til å beskrive "trusselformelen" i en åpent tilgjengelig publikasjon. Vandepeer argumenterer for at den tradisjonelle tilnærmingen egner seg bedre til å beskrive kjente (militære) trusler fra statlige aktører, men kommer til kort i forhold til ikke-statlige aktører som terrorister, der problemstillingen snarere er å identifisere trusselaktøren. Et sentralt trekk ved hybride trusler er at en statlig aktør vil benytte stedfortredere eller andre ikke-sporbare metoder for å skjule sin tilknytning og skape forvirring, og derfor vil analytiske tilnærminger som er utviklet for ikke-statlige trusselaktører bidra til deteksjon. Vandepeer anbefaler tre tilnærminger for å supplere intensjon/kapabilitet-tilnærmingen:

- Sårbarhetstilnærmingen. Intensjoner og kapabiliteter vurderes alltid i relasjon til noe, om det er klart definert eller underforstått. Selv om sårbarhetsvurderinger er mer assosiert

[3] En risikokilde er en handling eller en hendelse som i seg selv eller i kombinasjon med andre elementer kan lede til spesifikke, som regel uønskede, konsekvenser (SRA 2015:10).

med risikoanalyse, vil man ved å legge mer vekt på sårbarheter hos referanseobjektet (det som trues) få en mer fullstendig forståelse av trusselen (Vandepeer 2011:140-141).

- Miljøtilnærmingen. Trusselaktør og referanseobjekt settes inn i en bredere kontekst – *security environment*, som består av dimensjonene rom, tid og kontekst. En dypere forståelse for "sikkerhetsmiljøet" kan øke muligheten for å påvirke situasjonen uten å ha konkret kunnskap om konkrete trusselaktører (Vandepeer 2011:153).
- Situasjonstilnærmingen tar utgangspunkt i trusselaktøren som individ, og stille spørsmål ved om det er en rasjonell kalkyle som ligger bak ondsinnede handlinger, eller om det finnes bestemte situasjoner eller betingelser som gjør dette mulig (Vandepeer 2011:162). En situasjonstilnærming kan være til hjelp i kontraetterretning for å avdekke hvilke betingelser som må være til stede for at en person blir en innsidetrussel.

Hybride trusler utnytter identifiserte sårbarheter i ulike sektorer for å oppnå synergieffekt (DSB 2017), derfor er kunnskap om egne sårbarheter viktig for deteksjon. I tillegg vil forståelse av konteksten og den aktuelle situasjonen bidra til forståelse av hvilke effekter som ønskes oppnådd, selv om trusselaktøren ikke er identifisert.

Trusselpersepsjon og innflytelse på politiske veivalg

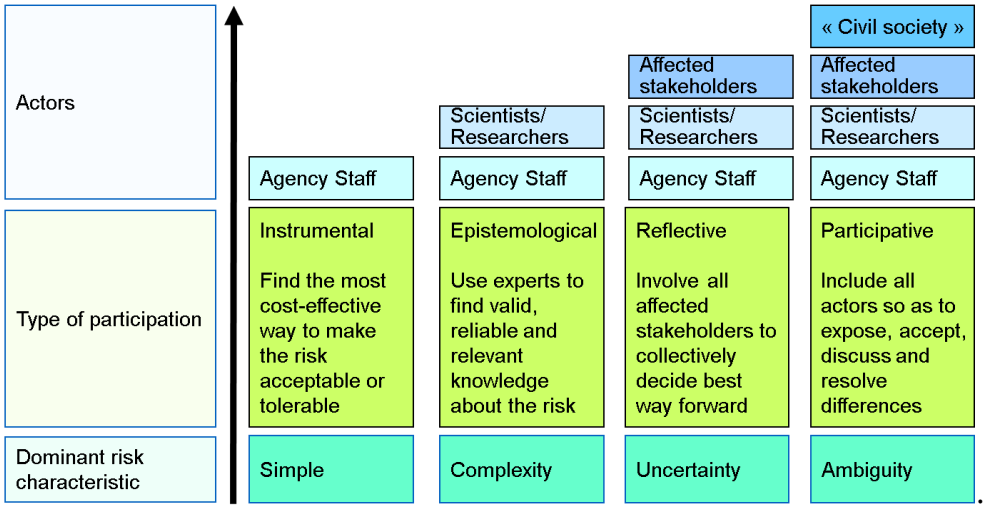
I følge Foley (2009:440) vil trekk ved (eller endringer i) det objektive trusselmiljøet kun påvirke en organisasjons policy i den grad i den grad trekkene eller endringene oppfattes av organisasjonen. Hypotesen er dermed at en organisasjons eller en stats sikkerhetstiltak er en funksjon av trusselpersepsjon og trusselnivå. Man kan si at trusselpersepsjon kan måles ut fra tre indikatorer: trusselaktørens kapabilitet, nærhet til trusselaktøren og trusselaktørens antatte intensjoner. Denne tilnærmingen kan forklare hvordan stater reagerer ulikt på trusler. Oppfatningen av nærhet kan for eksempel forklare hvorfor en stat som er truet av terrorister basert i utlandet reagerer annerledes enn en stat med et internt terrorismeproblem[4] (Foley 2013:46), eller hvorfor Norge opplever den militære trusselen fra Russland som høyere enn for eksempel Storbritannia (Widerberg 2017:27). I tillegg til trusselpersepsjon vil samfunnsmessige

[4] Kontraterror i USA handlet etter 2001 primært om å holde trusselen borte fra 'Fortress America', mens europeiske land behandlet terrorisme mer som et internt problem, ikke bare fordi mange land ikke ønsket å delta i en kinetisk 'war on terror', men også fordi EU manglet en helhetlig utenrikspolitisk dimensjon (Aldrich 2009:122).

normer (Foley 2013:51) og formelle regler, operasjonsprosedyrer og normer som styrer relasjonene mellom sikkerhetsinstitusjoner ha betydning (*ibid.*:66). De norske prinsippene for krisehåndtering og arbeid med samfunnssikkerhet er et eksempel på slike regler, normer og prosedyrer. I utenriks- og sikkerhetspolitisk sammenheng vil også statens opplevde utenrikspolitiske handlingsrom, de handlingsalternativene som er politisk mulige og operativt tilgjengelige for den strategiske ledelsen (Fermann 2010:32).

Stakeholder involvement model

Renn's stakeholder involvement-modell beskriver hvordan risiko håndteres ulikt basert på om risikoen grunnleggende sett er enkel, kompleks, usikker eller tvetydig. Jo lenger til høyre i modellen man beveger seg (og kunnskapsnivået om risikoen blir dårligere), jo større er behovet for å involvere flere aktører i håndteringen av risikoen. I tillegg til utfordringer knyttet til involvering og kommunikasjon, kan modellen også brukes til å illustrere spenningen mellom sentralisering og desentralisering på sikkerhetsfeltet.



Figur 1: Stakeholder involvement-modellen

Van Asselt og Renn (2011:436) peker på at selv om mange risikoer blir behandlet som om de var enkle, selv om de i virkeligheten inneholder kan beskrives som systemiske, det vil si at de er forplantet i en større kontekst av samfunnsmessige prosesser. OECD (2003:103) bruker moderne terrorisme som eksempel på en systemisk risiko. Fenomenet er vanskelig å definere, vanskelig å kvantifisere med historiske data og globalt i den forstand at hensikten er å ramme "det vestlige

systemet" via et nærmest uendelig antall mål og ved hjelp av et minst like stort antall angrepsmetoder. Etterretning er grunnleggende for å forstå trusselen og dermed informere den videre risikoanalysen (*ibid.*:2005).

Systemiske risikoer krever en helhetlig tilnærming for å identifisere, vurdere og håndtere farer og trusler. De er preget av avhengigheter mellom systemer eller sektorer, og man kan ikke vise til lineære årsak/virkningskjeder. Tvetydighet er ved siden av kompleksitet og usikkerhet en hovedutfordring ved risikovurderinger (Renn 2006:77).

Ifølge Gibson (2004:18) kan risikoens kompleksitet i stor grad håndteres av vitenskap og teknologi, mens usikkerhet og tvetydighet er utfordringer som i større grad må håndteres gjennom risikokommunikasjon. Kommunikasjon er et tillitsskapende tiltak som består i at private aktører eller offentlige myndigheter ikke bare forteller publikum at de vurderer og behandler risikoen, men at de også offentliggjør risiko som de identifiserer. Kompleksitet er knyttet til risikoens objektive virkelighet, mens tvetydighet og usikkerhet er knyttet til risiko som en sosial konstruksjon. Tvetydighet handler om at selv om man er enige om data og metoden for å måle dem, er det er debatt rundt hva resultatene egentlig betyr. Debatten rundt genmodifisert mat er et eksempel på slik tvetydighet. Usikkerhet handler om problemer knyttet til å kvantifisere konsekvenser og manglende evne til å måle sannsynlighet, for eksempel terror-risikoen (*ibid.*).

Tvetydighet er et sentralt trekk ved hybride trusler (Reichborn Kjennerud og Cullen 2016:2). Tvetydighet oppnås blant annet gjennom villeding, psykologiske- og informasjonsoperasjoner som bidrar til Clausewitz´ "*fog of war*" og vanskeliggjør respons (Davis 2015:22). Trusselaktøren vil handle fordekt, det kan være vanskelig å attribuere trusler eller angrep til en bestemt stat. Hybride trusler utfordrer binære forestillinger om krig/fred, militære og ikke-militære virkemidler, konvensjonelle og irregulære metoder (Hoffman 2007). Dette bildet vanskeliggjør beslutningsprosessen hos forsvareren. Giegerich (2016:69) peker på at beslutninger på nasjonalt nivå og oppgavefordeling mellom internasjonale organisasjoner som EU og NATO er komplisert. Avverging av og forsvar mot hybride trusler vil måtte involvere nasjonale og lokale myndigheter, internasjonale partnere, privat sektor, og kanskje samfunnet som helhet. Samtidig krever det minimal fantasi å se at behovet for bred involvering kan komme

i konflikt med behovet for å skjerme sensitiv informasjon knyttet til sikkerhetspolitiske vurderinger og etterretning.

I tillegg har det i norsk kontekst vist seg komplisert å realisere en *whole of-government*-tankegang i praksis gjennom for eksempel å utvikle organisering som kan ivareta både politiske og faglige hensyn. Integrasjonen mellom politisk og militær ledelse av Forsvaret er et eksempel på dette. Dersom det er utfordrende å etablere mer helhetlig tenkning i en enkeltsektor, vil utfordringene være tilsvarende større mellom sektorer, mellom statlige og ikke-statlige virksomheter og ikke minst på tvers av landegrenser (Bjerga 2010:127).

Samfunnssikkerhet og statssikkerhet

Hybride trusler er en utfordring både fra et samfunns- og statssikkerhetsperspektiv. Dette kommer til uttrykk gjennom måtene en trusselaktør kan utnytte svakheter i det norske forvaltningsapparatet, som er preget av sterke fagdepartementer, relativt selvstendige offentlige organisasjoner og svak samordning på tvers av sektorer og nivåer (Fimreite et. al. 2011:9). Det er derfor nødvendig å gi en kort beskrivelse av disse to aspektene av sikkerhet.

Samfunnssikkerhet ble først definert i St. meld. nr. 17 (2001-2002) som "den evne samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger" (JPD 2002:4). Utgangspunktet for analysen er definisjonen til Kruke et. al. (2005:10) som sier at en hendelse som truer samfunnssikkerheten må ha en eller flere av følgende karakteristikker: 1) fører til ekstraordinære påkjenninger og tap, (2) har høy kompleksitet og gjensidig avhengighet mellom offentlige organisasjoner og (3) har potensiale for å undergrave tillit til vitale samfunnsfunksjoner. Hendelsene som beskrives i scenarioene vil typisk besitte alle tre kjennetegn. Statssikkerhet eller nasjonal sikkerhet har mange mål til felles med samfunnssikkerhet, men har i større grad et territorielt og sikkerhetspolitisk fokus, som forsvar av nasjonale grenser og statsinstitusjoner (Olsen et. al. 2007:74). Langtidsplanen for forsvarssektoren definerer statssikkerhet som å "[...] ivareta statens suverenitet og integritet, samt å sikre politisk handlefrihet. Begrepet inkluderer også Norges bidrag til kollektivt forsvar utløst av NATO-traktatens artikkel 5" (FD 2016:17).

FD (2017a:32) konstaterer i sin stortingsproposisjon om ny sikkerhetslov at både eksterne og interne utviklingstrekk gjør det stadig vanskeligere å trekke et klart skille mellom statssikkerhet og samfunnssikkerhet. Dette er knyttet til det stadig mer komplekse og uforutsigbare trusselbildet, eksemplifisert med hybride trusler, som består av et bredt spekter av virkemidler og dermed gjør det vanskelig å spore og dokumentere hvem som står bak et angrep. Dermed blir det vanskelig å vurdere om trusselen hører inn under justis- eller forsvarssektoren. Videre har den teknologiske utviklingen ført til økte gjensidige avhengigheter mellom militær og sivil sektor, noe som illustreres gjennom det nye totalforsvarskonseptet, der Forsvaret i langt større grad enn tidligere er avhengig av støtte fra sivilsamfunnet og næringslivet (FD 2015a). Dermed er god samfunnssikkerhet også en faktor som påvirker Forsvarets evne til å ivareta statssikkerheten (FD 2016:47). Dette fører samtidig til et mindre tydelig skille mellom stats- og samfunnssikkerhet, og departementet foreslår derfor at lovens formål skal være å trygge *nasjonale sikkerhetsinteresser*, noe som medfører en utvidelse av virkeområdet til å gjelde mer enn statssikkerhet i snever forstand, samtidig som det understrekes at loven "[...] ikke skal være en bred samfunnssikkerhetslov (FD 2017a:32).

Hybride trusler utnytter bevisst gråsoner mellom vår oppfatning av krig og fred, sivil og militær sektor, og utfordringen for norske myndigheter vil trolig i stor grad handle om å avgjøre om man befinner seg i samfunns- eller statssikkerhetsdomenet. Forslaget til ny sikkerhetslov ser ut til å ta disse utfordringene inn over seg. Loven er ment å være en dynamisk og fleksibel rammelov som trekker de store linjene, og som forutsettes utfylt av mer detaljerte forskrifter (FD 2017a:15).

3.1.2 Krisehåndtering og etterretning

En hybrid trussel kan i verste fall manifestere seg i form av en sikkerhetspolitisk krise. Kriser, spesielt innen security-feltet, vil alltid ha en politisk dimensjon (Boin et. al. 2005, Kruke 2012:15). Evnen, eller snarere viljen til å erkjenne at man blir utsatt for en hybrid kampanje handler til syvende og sist om en politisk vurdering. Den hybride kampanjen vil også ofte ha som mål å svekke denne viljen, for eksempel ved å så splid eller nære opp under motsetninger i den politiske ledelsen eller mellom allierte. Litteraturen om krisehåndtering fokuserer i stor grad på patologier i beslutningsprosessen (organisatoriske og kognitive faktorer). Etterretning spiller en

sentral rolle i deteksjon og vurdering av trusler, og derfor er etterretningens funksjon og utfordringer i de ulike fasene av krisehåndtering et sentralt tema.

En krise handler om nøkkelordene *sentrale verdier, usikkerhet, tidspress* og *kritiske beslutninger* (Olsen et. al. 2008:47, Boin et. al. 2005:2):

1. En følelse av at sentrale verdier står på spill. Verdiene kan være trygghet, sikkerhet, ressurser eller nasjonal suverenitet.
2. En følelse av usikkerhet. Hva er krisens årsak, omfang og konsekvens?
3. Behov for rask handling. En beslutningstager vil ikke ønske å fremstå som handlingslammet. Dette er en faktor om i seg selv kan være krisedrivende ved at man handler overilt på dårlig grunnlag.

Ulykker, kriser og katastrofer er ikke det samme, selv om begrepene gjerne brukes om hverandre i dagligtale og i media (Olsen et. al. 2008:48). En hensiktsmessig inndeling kan være å ta utgangpunkt i hvilke ressurser som kreves for å håndtere fenomenet. Ulykker kan håndteres rutinemessig med de ressursene som har dette som hovedoppgave (blålysetatene). Dersom hvilende beredskapsressurser som for eksempel Røde Kors må trekkes inn, kan vi snakke om en krise. Og dersom aktører som ikke involveres til vanlig (transportfirmaer, direktorater og politisk nivå) må mobiliseres, kan man snakke om en katastrofe (*ibid.*).

Kriser handler også om persepsjon. Det såkalte Thomas-teoremet slår fast at ”If men define a situation as a crisis, then it will be a crisis in its consequences” (Kruke 2012:7). Kriser og katastrofer kan true samfunnsinstitusjoner, kulturelle og moralske verdier og dermed samfunnssikkerheten dersom befolkningen mister tillit til de institusjonene som skal ivareta kritiske funksjoner i samfunnet (Olsen et. al. 2008:60).

Kruke (2012:8) deler kriser inn i tre grunnleggende faser: en førkrisefase, den akutte krisefasen og etterkrisefasen. Inndelingen er sirkulær, ikke lineær, fordi vi når krisen er avsluttet vil vi befinne oss i en ny normaltilstand, en ny førkrisefase, der vi forhåpentligvis har lært av krisen vi har vært gjennom:

Figur 2: Krisens tre faser (Kruke 2005:8)

Boin et. al. (2005) peker på fem faser i håndteringen av en krise i akuttfasen. Fase 1, 2 og 5 er mest sentrale for problemstillingen i denne oppgaven:

1. Sense making. I denne fasen forsøker beslutningstagere å få danne seg et bilde av hva som skjer mens hendelsene pågår. Tilgjengelige løpende og grunnleggende etterretninger[5] og annen informasjon knyttet til krisen blir gjennomgått. Siden krisen kommer uventet, er det som regel ikke nok tilgjengelig etterretning McCarthy 1998:26). Trusselpersepsjon avgjør hvordan krisen vurderes å virke inn på våre verdier og målsetninger (McCarthy 1998:9). Faktorer som vanskeliggjør sense making-fasen blir diskutert i avsnittet "Å gjenkjenne trusselen".
2. Decision making. Risikoanalyse understøtter beslutningene om hvordan vi skal respondere på krisen. Ulike alternativer vurderes ut fra hvilke kostnader de forventes å ha internt og hvilke reaksjoner de vil føre til i det eksterne miljøet. Etterretningsfunksjonens viktigste innspill til risikoanalysen er å vurdere motpartens reaksjoner på våre mottiltak, samt å hjelpe beslutningstagerne til å forstå kompleksiteten i situasjonen (McCarthy 1998:9, 28-30). Selv om en rekke funksjoner vil bidra i risikoanalysen, er det som regel en enkelt person, en politisk leder, som står for det endelige valget av handlemåte (Boin et. al. 2005:43). En krise leder gjerne til ad hoc organisering av nye organisatoriske strukturer, også kalt *task-force*-fenomenet (McCarthy 1998:26). Mindre krisehåndteringsgrupper blir gjerne nav i større tverrsektorielle nettverk. Selv om slik

[5] Løpende etterretninger (*current intelligence*): Etterretninger som reflekterer den nåværende situasjonen på strategisk eller taktisk nivå. Til sammenligning utgjør grunnleggende etterretninger (*basic intelligence*) referansegrunnlaget for planprosesser og en basis for å tolke ny etterretning og informasjon (AAP-6).

organisering kan ha sine fordeler gjennom økt intellektuell og kognitiv kapasitet, kan de også lett bli offer for uheldige gruppedynamikker, enten for mye konflikt eller for mye konformitet (Boin et. al. 2005:46). For etterretningsfunksjonen kan det by på utfordringer dersom krisegruppen overtar analysen av informasjon og etterretninger. Mangel på kontakt med de som tar beslutningene kan ha en negativ effekt på styring/prioritering av etterretningsressurser samt analyse og kommunikasjon av etterretninger (McCarthy 1998:26).

3. Meaning making. Denne fasen handler primært om politisk kommunikasjon der beslutningstagerne definerer krisens natur for omverdenen.
4. End games. Denne fasen omfatter terminering av krisen
5. Learning. Består av læring fra hendelsen, forbedring av strategier og systemer, som leder inn i en ny førkrisefase. Det finnes heldigvis få eksempler på nasjonale kriser av dette omfanget i Norge som kan være grunnlag for læring og forbedring, med unntak for terrorangrepene 22/7 2011, som har ledet til en rekke forbedringspunkter[6]. Albrechtsen et. al. (2017:5) registrerer blant annet økt risikoerkjennelse i samfunnet og blant aktører innen samfunnssikkerhet og beredskap, samt høyere bevissthet om viktigheten av å prioritere hendelser med lav sannsynlighet og store konsekvenser etter 22/7.

Selv om kriser er preget av en grunnleggende usikkerhet, vil både forløpet og håndteringen preges av i hvilken grad myndigheter og andre aktører er forberedt (Olsen et. al. 2008:61). t´Hart og Boins typologi illustrerer hvordan kriser utvikler seg over tid: raskt/øyeblikkelig eller langsomt/krypende og hvordan de avsluttes: raskt/plutselig eller langsomt/gradvis (Olsen et. al. 2008:64). Mennesker oppfatter kriser på ulik måte, og samme hendelse kan for noen fremstå som en krypende krise som man har sett utvikle seg over tid, mens andre blir klar over problemet først når det har utviklet seg til en akutt krise (Boin et. al. 2005).

[6] En oversikt med status over de 71 tiltakene etter 22/7 er inkludert i Meld. St. 10 (JBD 2016:185)

		Krisens utvikling	
		Raskt, øyeblikkelig	Langsomt, krypende
Krisens avslutning	Raskt, plutselig	Hurtigbrennende kriser: flyulykker der årsaken finnes, gisseldrama som løses raskt og effektivt (Entebbe 1976).	Rensende kriser: Utvikler seg raskt og avsluttes langsomt (eks. tsunami, jordskjelv)
	Langsomt og gradvis	Lange skyggers kriser: skandalepregede hendelser som fører til dyptgående endringer	Krypende kriser: lavintensive konflikter, miljøproblemer, sult eller visse typer epidemier

Figur 3: typologi over kriser og katastrofer (Olsen et al 2008:64)

I forhold til typologien kan man se for seg et cyberangrep der strømmen slås av eller banktjenester blir utilgjengelige som intense og smertefulle, men like vel hurtigbrennende kriser, dersom omfanget ikke er større enn hva systemet eller samfunnet klarer å håndtere. Dersom omfanget blir for stort eller responsen ikke er tilpasset trusselen, kan angrepet bli en lange skyggers krise med konsekvenser langt inn i fremtiden, eksemplifisert gjennom USAs reaksjon på terrorangrepene i 2001 (Rothkopf 2014:47). Det samme gjelder dersom det viser seg at et isolert angrep er del av en større kontekst, for eksempel en hybrid trussel fra en statlig aktør. Utenlandsk etterretningsvirksomhet/spionasje og påvirkningsoperasjoner som foregår i det skjulte, vil være vanskeligere å detektere, og ligner mer på en krypende krise. Utfordringen med krypende kriser er at de egentlig ikke blir en krise før de er politisk definert som en krise, som for eksempel miljøproblemer, sultkatastrofer eller AIDS-epidemien. De er heller ikke over før politikere "vedtar" at krisen er avsluttet (Olsen et. al. 208:64). Parallellen til hybride trusler og hybridkrig er åpenbar: Ukrainas og Vesten respons mot den russiske overtagelsen av Krym i 2014 ble vanskeliggjort gjennom tvetydigheten som oppstod da umerkede spesialsoldater ble deployert på halvøya. Det ble vanskelig å "vedta" politisk at dette var en invasjon. Informasjonsoperasjoner som skapte inntrykk av at dette var lokal milits bidro til mer tvetydighet og forvirring med dårlig trusselforståelse som resultat. Dette vanskeliggjorde respons ytterligere (Giles 2016:32)

3.1.3 Å gjenkjenne trusselen

Dette avsnittet omtaler teori som beskriver årsaker til at farer eller trusler ikke blir oppfattet, og deretter mer optimistisk anlagt teori som med peker på måter organisasjoner kan motvirke disse destruktive tendensene. Disse teoribidragene handler grunnleggende sett om organisatorisk design og om sikkerhetskultur. Det legges til grunn at organisasjonsteoretiske prinsipper også er relevante på samfunnsnivå, det vil si mellom etterretnings- og sikkerhetsinstitusjoner og beslutningstagere på departements- og politisk nivå. Barry Turner (1976) peker på faktorer som gjør at organisasjoner ikke klarer å oppfange signalene om at en fare truer. Boin et. al. (2005) går dypere inn i organisatoriske og politiske årsaker til at kriser ikke blir gjenkjent som det de er. Studier av High Reliability Organizations (HRO) viser måter disse hindringene kan bekjempes.

Etterretningsfadeser og organisasjonsfeil

Både risikostyring og etterretningsstudier fokuserer på hvordan prosesser og organisasjoner kan forbedres for å unngå at feil skjer, enten ved at en tilsiktet uønsket handling ikke fanges opp tidsnok, eller ved at en industriulykke inntreffer. Det finnes like vel få eksempler på "krysskobling" mellom de to fagområdene. En fullstendig sammenstilling av teori fra henholdsvis etterretningsstudier og risikostyring vil av plasshensyn ikke være mulig her, selv om det kunne vært en interessant studie i seg selv.

Deteksjon av trusler handler om indikasjon og varsling, etterretningens kjernefunksjon: "Nothing is more important in the world of intelligence than preventing surprise" (Hulnick 2005: 593). Dunn Cavelty og Mauer (2009:129) skiller mellom to typer av varsling. På den ene siden finnes tradisjonell *monitorering* av identifiserte parametere som allerede er klassifisert som mulige trusler. På den andre siden har man *discovery*, eller støtte til beslutningstagere for å identifisere mindre åpenbare farer som kan inntreffe. Her er det relevant å påpeke forskjellen mellom konseptene trussel og risiko: Risiko er det som *kan skje*, ikke det som allerede *foregår* (Dunn Cavelty et.al 2011:6). Trusler kan dermed monitoreres, mens risiko hører hjemme i *discovery*-domenet. Deteksjon av at man er utsatt for en hybrid trussel og ikke en rekke tilfeldige hendelser handler om å detektere at hendelsene er koordinert, og at det ligger en politisk intensjon bak dem. Manglende deteksjon av en strategisk trussel vil gjerne bli kalt en etterretningsfadese (*intelligence failure*). Typiske årsaker kan være mangel på informasjon

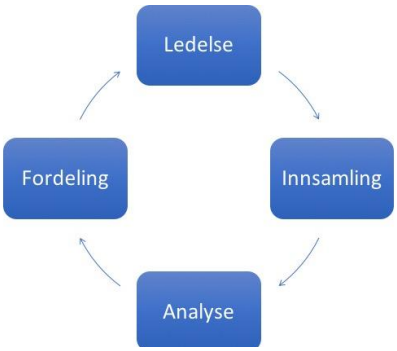
(manglende eller irrelevant innsamling), kognitive heurestikker[7] som leder til feilslutninger i analysefasen. Det finnes en rikholdig litteratur på etterretningsfadeser, mye fra fagområdet etterretningsstudier (Handel 2003, Kuhn 2003, Bar-Joseph 2003, Hatlebrekke og Smith 2010). De ulike kognitive faktorene som ligger til grunn for at etterretningsanalyse kan lede til feil slutninger blir ikke drøftet videre her, men det er på sin plass å konstatere at dette alltid vil være en utfordring for deteksjon og varsling.

Konsekvensen av en etterretningsfadese eller et strategisk overfall er gjerne økte investeringer i innsamling eller kostbare reorganiseringer (Bar-Joseph 2005:176). Samtidig er det en ny trend at virksomheter i privat sektor som sitter på for eksempel finansielle eller sosiale data i økende grad blir ansvarlige for deler av etterretningsinnsamlingen gjennom «outsourcing» av denne funksjonen, som tidligere var statlige organisasjoners eksklusive domene (Petersen og Tjalve 2017:3). Rathmell (2002:99) minner om at globalisering, IKT-revolusjonen og det generelt mer dynamiske trusselbildet også har ført til at etterretningstjenester har mistet informasjonsmonopolet de var vant til å ha under den kalde krigen til fordel for mer horisontale kunnskapsnettverk (*ibid*.). Kunnskapen må søkes der den finnes, og dermed bør man legge til rette for økt samarbeid med privat sektor, forskningsinstitusjoner etc. Informasjon fra åpne kilder (open source intelligence/OSINT) spiller en særlig viktig rolle for å holde en bredere gruppe av interessenter og samfunnet for øvrig informert og involvert.

Studier av strategiske overfall viser på sin side at det kun er unntaksvis at forsvareren er helt uten forvarsel. Feilen ligger, ved siden av allerede nevnte feil i analysen, ofte i beslutningstagerens tolkning av informasjonen (Riste 2007:525). Herman (1996:45) hevder også at ”dissemination tends to be intelligence’s Achilles’ heel”. Avstanden mellom produsenter og brukere er et punkt som tradisjonelt skaper debatt. For stor nærhet kan true etterretningens integritet og lede til politisering av det endelige produktet. For stor avstand kan gjøre produktet mindre relevant for

[7] Typiske heurestikker som kan være en utfordring i etterretningsarbeid kan være at man kun får øye på det man forventer å finne, man ser kun etter bevis som bekrefter en hypotese, ikke avkrefter den, og at man ubevisst fyller inn manglende data med sine egne erfaringer. Etnosentrisme vil også spille inn og påvirke måten signalene tolkes på (Dunn Cavelty og Mauer 2009:132).

brukeren (Betts 2003:61). Det spiller også en rolle om beslutningstagerne mottar et omforent produkt, slik tilfellet er i Storbritannia, der Joint Intelligence Committee sammenstiller bidrag fra de ulike tjenestene, eller om bidragene kommer ukoordinert i separate kanaler, slik som i USA[8] (Arntsen 2010:135).



Figur 4: Etterretningshjulet

Også fagområdet risikostyring har en rekke relevante teoretiske perspektiver. Reason (1997:195) har et optimistisk syn på at en sikker organisasjon kan formes. Perrow er på sin side langt mer skeptisk til at det går an å få komplekse systemer til å fungere på en sikker måte. Han skiller mellom lineære og komplekse systemer på den ene siden og tett og løs kobling på den andre. Komplekse systemer med tette koblinger er mest utsatt for det han kaller systemulykker, der flere mindre feil i systemet interagerer på en uventet måte (Perrow 1984:70). Etterretningsfadeser kan også forstås som *normal accidents* i store komplekse systemer. Når etterretningsorganisasjoner feiler i sitt oppdrag kan det skyldes eksterne årsaker som et uforutsigbart og fiendtlig trusselmiljø. Det kan også skyldes interne årsaker som kognitiv eller motivasjonsmessig utilstrekkelighet hos enkeltindivider, feil i organisasjonsdesign og feil prioriteringer eller manglende oppmerksomhet på ledelsesnivå (Perrow 2011:291). Perrow peker også på at organisasjonsfeil lett vil oppstå dersom standarder eller regulering mangler eller ikke blir fulgt opp (*ibid.*:295). En vanlig, men lite konstruktiv respons på organisasjonsfeil er gjøre koblingene tettere og å øke, i stedet for å redusere kompleksiteten. Dette kan være nye og tidkrevende prosedyrer eller nye lag av ledelse (og byråkrati). Perrow (2006) bruker reformene i

[8] De amerikanske etterretnings- og sikkerhetstjenestene, US Intelligence Community (USIC), har også produsert flere ugraderte fellesprodukter i den senere tid, for eksempel vurderingen av russisk innblanding i presidentvalget i 2016 (DNI 2017).

de amerikanske systemet etter terrorangrepene 11. september 2001 som eksempel. Strømlinjeforming av komponentene, læring, ansvar og eierskap til de ulike delene av etterretningsprosessen, samt evaluering av suksess på lik linje med feil kan være mer fornuftige responser (Hatch 2013:25).

Turners Failure of Foresight-teorien

Turner (1976:378) beskriver en del fellestrekk som ligger bak større katastrofer. Studien er basert på granskinger av tre større ulykker i Storbritannia på 1960 og 1970-tallet, der Turner kunne påvise at en *failure of foresight* hadde funnet sted, det vil si at foranstaltninger som i organisasjonskulturen har vært oppfattet som tilstrekkelige viste seg å ikke være det. Disse fellestrekkene inntreffer i inkubasjonsfasen, beskrevet av Turner som "the accumulation of an unnoticed set of events which are at odds with the accepted beliefs about hazards and the norms for their avoidance" (*ibid.*:381). Inkubasjonsfasen er tidspunktet der en trussel kan detekteres:

- Institusjonelle fordommer
    - Alle organisasjoner utvikler en kultur som på den ene siden bidrar til effektivitet, men som på den andre siden kan føre til kollektiv blindhet (Turner 1976:388). Forbindelsen mellom makt og offisielt godkjent kunnskap er særlig relevant, siden beslutningstagere har stor innflytelse på hvordan deres underordnede oppfatter miljøet og organisasjonen de fungerer i. Slike begrensninger på hvordan man skal tenke og oppfatte signaler kan ha katastrofale konsekvenser (Turner og Pidgeon 1997:3-4). Ledelsen har et særlig ansvar for hvilken organisasjonskultur som utvikles. Bar-Joseph (2005:167) viser hvordan autoritære og dogmatiske holdninger blant toppledelsen i israelsk militær etterretning var en sterkt medvirkende årsak til at varsler om et forestående angrep fra Egypt i 1973 (Yom Kippur-krigen) ikke ble varslet i rett tid.
- Avledning/distraksjon
    - I mange ulykker har det vist seg at de involverte tar tak i veldefinerte problemer eller farekilder, og dermed ignorerer farligere, men dårligere strukturerte problemer som skjuler seg i bakgrunnen (Turner 1976:388). De dårligere strukturerte problemene er gjerne preget av tvetydighet og usikkerhet (Pidgeon

2010:215). Distraksjon og avledning er et kjerneelement ved hybride trusler: manipulering av media gjennom «sjokkerende» bilder undergraver motstanderens legitimitet, anonyme cyberangrep og paramilitære styrker med uklart oppheng vanskeliggjør respons, og globale informasjonsoperasjoner skaper splittelse mellom allierte (Lasconjarias og Larsen 2017:10).

- Manglende evne til å høre på varsler
    - Organisasjoners iboende eksklusivitet kan føre til at utenforstående som kommer med varsel om en truende situasjon avfeies (Turner 1976:388). En bred involvering av interessenter, spesielt i forhold til komplekse og tvetydige risikoer som beskrevet i *Stakeholder involvement*-modellen kan motvirke denne tendensen. Tradisjonelt «lukkede» etterretningsmiljøer kan være spesielt utsatt for slik isolasjon, og derfor vil det være viktig å åpne for ekstern kunnskap gjennom horisontale nettverk på bekostning av den tradisjonelle horisontale integreringen (Dunn Cavelty og Mauer 2009:139).
- Problemer med informasjonshåndtering
    - Det finnes en rekke utfordringer ved informasjonshåndtering som fører til at informasjonen ikke er tilgjengelig når den behøves. Dårlig strukturerte problemer vil følges av informasjonsproblemer (Turner 1976:388). Problemene kan skyldes for mye informasjon, informasjon i feil kanaler, ufullstendig informasjon, informasjon som oppfattes som lite relevant, dårlige informasjonskilder eller manglende evne til å koble sammen tilgjengelige data. (Turner 1976:388, Pidgeon 2010:214). Granskingen av terrorangrepene i USA i 2001 viste at det fantes tilgjengelig og relevant informasjon hos både CIA, NSA og FBI, men at denne aldri ble koblet sammen i tilstrekkelig grad, slik at man kunne se det totale bildet av trusselen (9/11 Commission 2004:254-277).
- Utenforstående bidrar til å gjøre situasjonen verre
    - Hos Turner representerer ”utenforstående” publikum som på en eller annen måte griper inn i en farlig prosess eller ulykke, gjerne med de beste hensikter, men som på grunn av manglende kunnskaper bidrar til å forverre situasjonen (Turner 1976:390). I en analyse av hybride trusler vil de ”utenforstående” representere

publikum som for eksempel blir utsatt for en påvirkningsoperasjon eller media som uforvarende videreformidler falske nyheter.

- Lovpålagte krav følges ikke
    - I Norge har NSM gjennom flere år rapportert at sikkerhetstilstanden (forholdet mellom risikobilde og forebyggende sikkerhet) ikke er tilfredsstillende, og at gapet mellom trusler og sikkerhetstiltak er økende (Elgsaas og Heireng 2014:7). Årsakene er både menneskelige, organisatoriske og tekniske, men basert på NSMs tilsynsrapportering dominerer de organisatoriske årsakene som for eksempel ledelsens fokus på sikkerhet, kompetanse, dokumentasjon og oversikt, rutiner og rapportering, manglende reaksjoner på brudd og mangler i regelverk (*ibid.*:42-64). Gjørv-kommisjonen påpekte også manglende evne til å gjennomføre det man har bestemt, evne til koordinering, evne og vilje til å klargjøre ansvar og treffe tiltak som til sammen førte til alvorlig svikt i beredskap og evne til å avverge og beskytte samfunnet mot trusler (Statsministeren 2012:450).
- Åpenbare farer ignoreres
    - Ifølge Gjørv-kommisjonen er det risikoforståelsen som «ligger til grunn for hvilke tiltak som iverksettes, og er dimensjonerende for den sikkerhet og beredskap samfunnet velger å ha» (Statsministeren 2012:451). Selv om trusler detekteres og varsles i rett tid, er det ingen garanti for at dette leder til de rette beslutningene. Det britiske Underhuset mottok en rapport i 2009 som advarte mot trusselen Russland utgjør for tidligere Sovjet-stater, der det blant annet ble påpekt at marinebasen i Sevastopol på Krym-halvøya var spesielt utsatt for militær intervensjon (Giles 2016:61). Manglende risiko- og trusselforståelse er svært komplekst, og henger blant annet sammen med mengden av informasjon som er tilgjengelig og evnen til å skille «signaler» fra «støy» i øyeblikket og menneskers evne til å bortforklare ny informasjon som bryter med normalen og plassere denne inn i vante tankesett (Boin et. al 2005). I forordet til *Pearl Harbor – Warning and Decision* (Wohlstetter 1962:vii) skriver Thomas C. Schelling at «There is a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered seriously looks strange; what looks strange is thought improbable; what is improbable need not be considered seriously».

High Reliability Theory

Studier av såkalte High Reliability Organizations (HRO) representerer et positivt syn på sikkerhetskultur, og peker på mulige løsninger på de utfordringene som reises av Turner. HRO-teorien er basert på undersøkelser av organisasjoner innen forsvar, luftfart og kjernekraft som opererer høyrisikosystemer med lav ulykkesprosent.

En HRO er preget av at ledelsen konsistent prioriterer sikkerheten høyt (Sagan 1993:17). Kortsiktig effektivitet eller profitt kommer på andreplass. De legger vekt på høy grad av redundans i sine systemer (*ibid.*:21). Risikoen for feil i enkeltkomponenter eller menneskelige feilgrep reduseres gjennom desentraliserte beslutninger og en sterk organisasjonskultur, der alle ansatte sosialiseres inn i en kultur som vektlegger sikkerhet og pålitelighet. Kontinuerlig operasjon og trening sørger for at operatører ikke "glir inn" i rutinemodus med påfølgende senket årvåkenhet (*ibid.*:22-24). En HRO er også preget av stor evne til organisatorisk læring gjennom prøving og feiling (*ibid.*:25-26). Reason (1997:195) legger også vekt på informasjonsaspektet, og understreker videre fleksibilitet, evne til å tilpasse seg endrede krav (*ibid.*:213).

Westrum og Adamski (1993) og Rasmussen (1997) legger som Reason vekt på at måten en organisasjon prosesserer informasjon er en viktig faktor for å bygge en sikkerhetskultur. Rundt ethvert sosioteknisk system finnes det mennesker som utvikler, opererer, vedlikeholder og evaluerer systemet. En organisasjons styrke avhenger av i hvilken grad den klarer å vedlikeholde dette menneskelige "sikkerhetsnettet" (Westrum og Adamski 1993:4). Effektiv kommunikasjon kan oppdage latente feil i et system (Westrum og Adamski 1993:18). Rasmussen (1997:196) understreker også at et kontrollsystem aldri blir bedre enn sin informasjonskanal. Informasjon om systemets reelle tilstand må gjøres tilgjengelig for alle aktører på et nivå og i en form som er relevant for den enkeltes oppgave, og man må klart definere hvor grensen for akseptabel risiko går. Dermed kan man hindre at systemet, gjennom en rekke isolerte avvik gjort av enkeltpersoner, beveger seg mot det punktet der en ulykke kan skje.

3.1.4 Delkonklusjon

Forholdet mellom en trussel- og en risikotilnærming til sikkerhet er drøftet i teorigjennomgangen. Begge tilnærminger handler om å redusere usikkerhet for

beslutningstagere, men trusseltilnærmingen handler i større grad om ting som allerede pågår, om epistemisk usikkerhet og jakten på informasjon som eksisterer, selv om den kan være vanskelig tilgjengelig. Risiko handler til sammenligning om mulige farer som ikke ennå har manifestert seg. Et varslingssystem trenger begge perspektiver.

Det er en strategisk utfordring å etablere systemer for varsling og krisehåndtering der fagnivået kobles med beslutningstagerne og dermed både sørger for relevant etterretning og varsling *og* at varslingen blir oppfattet. Det er også en strategisk utfordring å gjøre tverrsektorielt og offentlig samarbeid og informasjonsutveksling mulig, samtidig som operasjonssikkerhet ivaretas. På operativt nivå finner vi organisatoriske, kognitive og teknologiske utfordringer. I norsk kontekst er de organisatoriske utfordringene pekt på blant annet av Gjørv-kommisjonen. Også Traavik-utvalgets eksterne gjennomgang av PST etter 22. juli-angrepene fremhever "mangelfull ledelse, uhensiktsmessig organisering, lite effektive arbeidsprosesser" og en "statisk, tradisjonsbundet organisasjonskultur" (JBD 2012:3). På taktisk nivå er utfordringen å sette opp relevante indikatorlister og følge utviklingen på de identifiserte områdene basert på et rettidig tilfang av informasjon fra et bredt spekter av kilder, samtidig som man klarer å scanne horisonten for ukjente farer som *kan* inntreffe.

Trusselbildet etter den kalde krigen oppfattes som mer komplekst, preget av asymmetri og uforutsigbarhet. Hybride trusler passer inn i dette bildet på minst to måter. Først og fremst gjennom at skillet mellom virkemidler som tradisjonelt kan knyttes til enten statlige eller ikke-statlige aktører viskes ut, dernest gjennom at hybride trusler ikke krysser etablerte grenser for når det er legitimt å reagere militært, og dermed utfordrer forsvarerens risikopersepsjon og beslutningsprosesser. I Becks risikosamfunn må viktige beslutninger ofte treffes basert på et svakt kunnskapsgrunnlag, og beslutningene kan ha uante konsekvenser (Rasmussen 2001). Et effektivt forsvar mot hybride trusler må derfor basere seg på et risikokonsept som tar høyde for usikkerhet, enten denne usikkerheten handler om at man ikke har god nok innsikt i motstanderens planer og beslutningsprosesser, eller mer fundamental, ontologisk usikkerhet, knyttet til utilsiktede konsekvenser av tiltak som settes i verk.

For å håndtere risikoer preget av tvetydighet, kompleksitet og usikkerhet anbefaler Renn involvering av et bredt spekter av interessenter. For å detektere hybride trusler behøver vi å legge

til rette for tverrsektorielt samarbeid mellom sikkerhetsinstitusjoner (for eksempel mellom forsvars- og justissektoren), samarbeid mellom offentlige myndigheter og privat sektor (spesielt der kritisk infrastruktur eies av private), samt involvering av sivilsamfunnet i sin helhet. Befolkningens evne til å motstå informasjonsoperasjoner og årvåkenhet overfor «falske nyheter» er et eksempel på det siste. På security-området, der vi står overfor tenkende trusselaktører som kan tilpasse seg våre sikkerhetstiltak, må imidlertid behovet for bred involvering avstemmes med behovet for å skjerme sensitiv informasjon.

Vår evne til å gjenkjenne en krise utfordres på flere nivåer, både kognitivt, organisatorisk og politisk. Teori om sikkerhetskultur og etterretningsfadeser er relevant for å forstå disse utfordringene. Komplekse systemer eller organisasjoner har en nærmest iboende evne til å generere feil ved at informasjon ikke når frem til rett sted til rett tid og ved at man ikke søker etter den rette informasjonen. Det finnes et motsetningsforhold mellom desentralisert beslutningsmyndighet på den ene siden, og behovet for operasjonsprosedyrer og sentralisert kommando og kontroll på den andre siden. HRO-teori viser viktigheten av situasjonsforståelse og informasjonsflyt for å kompensere for menneskelige feil og utfordringer på kognitivt, organisatorisk og politisk nivå.

3.2 Hybride trusler

Det følgende avsnittet vil innledningsvis vise ulike definisjoner av hybridkrig og hybride trusler og deretter definisjonen som legges til grunn i oppgaven. I et sosial-konstruktivistisk perspektiv er det viktig å vise ulike oppfatninger av fenomenet. Deretter gjennomgås perspektiver fra aktuell forskning på sentrale elementer ved hybride trusler, noe som gir grunnlag for den morfologiske analysen. Beslektede begreper presenteres deretter og settes i sammenheng med den valgte definisjonen av hybride trusler. Avslutningsvis oppsummeres trekk ved hybride trusler som skaper særlige utfordringer for deteksjon.

3.2.1 Definisjon

Begrepene "hybrid krigføring" og "hybride trusler" defineres på svært ulike måter av ulike observatører (Tuck 2017, Reichborn Kjennerud og Cullen 2016:1). Det er en merkelapp som beskriver mange forskjellige fenomener. Et fellestrekk ved mange definisjoner er at de

vektlegger en vestlig forståelse av krig som fokuserer på det kinetiske og teknologiske (Reichborn Kjennerud og Cullen 2016:1). De vestlige binære kategoriene krig og fred forutsetter at det eksisterer regler for hvordan krig skal utkjempes, som at de stridende bærer uniform og nasjonale kjennemerker, og at man forholder seg til internasjonal humanitær rett (Rinelli og Duyvesteyn 2017:22). Dette er en sårbarhet som hybride trusler utnytter. Clausewitz så på krig som en fortsettelse av politikken med andre midler, og mente at det kun er krigens spesielle virkemidler som skiller den fra politikk (Clausewitz 1873). Krig er i denne sammenheng mer enn å nedkjempe en motstander. I en videre forstand handler det om å få motstanderen til å handle på en ønsket måte.

Frank Hoffman tar utgangspunkt i kombinasjonen av ulike taktikker, med fokus på kinetiske/voldelige virkemidler: «Any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives" (Hoffman, 2014). Hoffman påpeker selv at definisjonen ikke tar høyde for ulike ikke-voldelige handlinger som bruk av stedfortredere, informasjonsoperasjoner, diplomatiske, økonomiske og juridiske tiltak (*ibid.*). NATOs toppmøte i Wales i 2014 definerte hybride trusler som "a wide range of covert and overt military, paramilitary and civilian measures […] employed in a highly integrated design" (NATO 2014). NATOs generalsekretær anerkjenner at hybride metoder ligner NATOs Comprehensive Approach, men med motsatt fortegn: "Hybrid is the dark reflection of our Comprehensive Approach. We use a combination of military and non-military means to stabilize countries. Others use it to destabilize them" (Stoltenberg 2015).

Hoffman (2017:3) påpeker at NATO opererer med langt bredere definisjoner av hybride trusler enn hva hans eget utgangspunkt var, og at de dermed kan brukes til å forklare nesten hvilken krig som helst. Deres hovedfokus er på kombinasjon av ulike metoder, integrasjon og "skreddersydd" design. Hoffman mener at NATOs syn på hybride trusler ligger nærmere det amerikanske kilder omtaler som "gråsonekonflikter" eller hans eget begrep "measures short of war" (*ibid.*).

Norske myndigheter fokuserer på statlige aktører i sin omtale av hybride trusler og hybrid krigføring. De legger vekt på at hybride trusler primært har som mål å destabilisere, og at

varsling og attribusjon er spesielle utfordringer. De norske definisjonene ligger nærmere NATOs syn, på den måten at de nevner en lang rekke ikke-militære og ikke-kinetiske virkemidler i tillegg til tradisjonell militærmakt. Statusrapporten fra Landmaktutredningen understreker økt oppmerksomhet om "ikke-militære og fordekte militære virkemidler som et viktig supplement til tradisjonell militær maktbruk [...]", og peker på særlige utfordringer for Norge gjennom at myndighetene kan settes uten press uten at det foreligger artikkel 5-situasjon, samt utfordringer knyttet til å forutse hvilke virkemidler som kan benyttes og hvor i landet de kan settes inn (FD 2017b:8). NSM definerer hybride trusler eller hybrid krigføring som "sammensatt bruk av militære og ikke-militære virkemidler" (NSM 2017:10). Bruk av militærmakt omtales som et "bakteppe", og er altså ikke en nødvendig komponent for å kunne snakke om en hybrid trussel i henhold til NSMs definisjon. NSM peker på vanskelighetene med å forstå målsetningen, hvem som er ansvarlig og i hvilken grad hendelser er sentralstyrte. Et viktig poeng er at pågående operasjoner kan være del av kapasitetsbygging, der intensjonen om bruk av disse kan oppstå på kort varsel (*ibid.*).

I denne oppgaven defineres statlige hybride trusler som *en stats vilje og evne til å benytte en kombinasjon av åpenlyse og fordekte militære og ikke-militære virkemidler koordinert i tid og flere dimensjoner (politisk, militært, informasjonsmessig, økonomisk, juridisk, fordekt) for å nå strategiske målsetninger, samtidig som den politiske risikoen for konvensjonell krig minimeres.* Definisjonen er dermed bredere enn Hoffmans syn på hybride trusler, og har mye til felles med det Mazarr (2015) omtaler som "gråsonekonflikter". En bred definisjon av er valgt for at den videre analysen i størst mulig grad skal reflektere norske myndigheters syn på hva en hybrid trussel består av. Det er heller ikke ønskelig å innføre enda et nytt begrep, selv om Ekspertgruppen for Forsvaret av Norge (FD 2015b:8) omtaler også sikkerhetspolitiske kriser som finner sted i *"en uklar gråsone mellom krig og fred"*.

3.2.2 Sentrale trekk ved hybride trusler

Hybridbegrepet slik det brukes i vestlige kilder, spesielt etter 2014, kan betraktes som forsøk på å kategorisere det man har observert av russisk aktivitet i Ukraina (Cederberg og Eronen 2015:3, Kofman og Rojanski 2015:1). I russiske kilder brukes begrepet først og fremst som en referanse til diskusjonen i Vesten (Renz og Smith 2016:8, Galeotti 2016a:24), og for å beskrive trusler som

russerne er opptatt av: Vestens utnyttelse av maktvakuumet som oppstod etter den Kalde krigen for å spre sin innflytelse i den post-sovjetiske sfæren, for eksempel sponsing av "fargerevolusjoner" i Georgia, Midtøsten og Ukraina (Perepelitsya 2015:418, Kofman og Rojansky 2015).

Den politiske målsetningen til statlige og ikke-statlige aktører som benytter hybride trusler er ifølge Hartmann (2017:2) å bevare eller etablere udemokratiske regimer og å øke egne strategiske opsjoner for å styrke sin makt i internasjonale relasjoner. Andre statlige aktører som bruker lignende metoder og som nevnes i litteraturen ved siden av Russland er først og fremst Kina og Iran, men også Brasil, Tyrkia og India. Disse har det til felles at de er land som er misfornøyde med sin regionale og globale innflytelse og egen evne til å sette dagsordenen. Dermed karakteriserer Mazarr (2015:11) dem som revisjonistiske regimer som har et ønske om å forandre status quo, men uten å gå til åpen konflikt med Vesten og USA.

Hybride trusler er strategiske av natur (Thiele 2016:3). Målet er å angripe motstanderens strategiske beslutningsprosess og/eller samholdet i sikkerhetsorganisasjoner som NATO. Å angripe fiendens strategi er et av prinsippene til den kinesiske strategen Sun-Tzu (Hartmann 2017:2)[9]. Det fysiske målet som blir angrepet trenger bare å ha en indirekte relasjon til den overordnede strategiske målsetningen (Ciluffo og Clark 2012:49).

Hybride trusler fra statlige aktører kjennetegnes av at alle statens virkemidler, militære og ikke-militære, integreres under en enhetlig nasjonal ledelse for å oppnå strategiske mål (Hartmann 2017:3). Maktbruk eller trusler om maktbruk spiller en sentral rolle. (Reichborn-Kjennerud og Cullen 2016:2). Samtidig forsøker trusselaktøren bevisst å viske ut grensen mellom de (vestlige) kategoriene krig og fred, gjennom at man hverken erklærer eller avslutter en krig (Hartmann

[9] «What is of supreme importance in war is to attack the enemy's strategy» [https://en.wikiquote.org/wiki/Sun_Tzu]. Cavanaugh (2014) peker på "Boycott, Divestments, Sanctions"-bevegelsen som et eksempel på et angrep på Israels strategi om å isolere palestinerne. Talibans infiltrasjon av afghanske sikkerhetsstyrker og et økende antall «green on blue»-angrep er et angrep på ISAFs strategi om å sette Afghanistan i stand til å ivareta egen sikkerhet, gjennom at alliansen bruker stadig mer ressurser på bakgrunnssjekker av afghansk personell.

2017:3). Det vil være vanskelig å slå fast nøyaktig når den organiserte voldsbruken når et nivå som tilsvarer det som defineres som "krig" (Cederberg og Eronen 2015).

Hybride trusler kan ses på som et substitutt for åpen militær maktbruk med den politiske risikoen dette innebærer (Chivvis 2017:2). Militære styrker i et hybrid scenario benyttes primært for å true andre stater og deres befolkninger, støtte egne sivile aktører og beskyttelse av eget territorium gjennom for eksempel truende øvelsesaktivitet og andre former for signalering. Et hyppig sitert eksempel er konseptet Anti-Access/Area Denial (A2AD)[10] og deployering av konvensjonelle høypresisjonsvåpen slik at man unngår direkte konfrontasjon og dermed risikoen for et strategisk nederlag (Hartmann 2017:3). Samtidig er det en kjensgjerning at en krig ikke kan vinnes med informasjonsoperasjoner og cyberangrep. Selv under anneksjonen av Krym, der Russland hadde fordelene av fullstendig informasjonsdominans, egne lokale militærbaser og en i stor grad vennligsinnet befolkning, var det nødvendig å sende inn spesialstyrker for å sikre et fait accompli (Galeotti 2016a:51).

Informasjonsoperasjoner og stedfortredere, for eksempel i form av politiske bevegelser i andre land brukes for å påvirke befolkninger og politiske ledere til å handle på måter som støtter trusselaktørens strategi, samtidig som man kontrollerer informasjonen som presenteres for egen befolkning (Hartmann 2017:3). Informasjonsoperasjoner handler ikke bare om å presentere sitt eget narrativ, men like mye om å forvirre det internasjonale publikum gjennom å publisere ulike narrativer som gjør det vanskelig å identifisere en objektiv sannhet (Chivvis 2017:3).

En vellykket hybrid kampanje krever først og fremst sterk politisk ledelse som gir mandat, samt evne og vilje til å dedikere nødvendig ressurser (Cederberg og Eronen 2015). Autoritære regimer med sterk sentral styring vil ha en fordel gjennom at de har større mulighet til å koordinere og styre bruken av ressurser fra ulike samfunnssektorer som diplomati, forsvar, medier, næringsliv i

[10] I en russisk kontekst vil det man i Vesten kaller A2AD inngå i en eller flere strategiske operasjoner på linje med cyberangrep, informasjonsoperasjoner og konvensjonelle styrker i den hensikt å øke eget handlingsrom og redusere egen risiko samtidig som motstanderens handlingsrom reduseres (Covington 2015:29).

en målrettet kampanje. Liberale stater kan også nasjonalisere økonomien og informasjonsdomenet, men da innenfor rammen av total krig (Dayspring 2015:30). Fraværet av ett sentralt koordineringpunkt i liberale demokratier vil dermed vanskeliggjøre respons (Galeotti 2016b:2, Reichborn-Kjennerud og Cullen 2016:2).

Gjennomføring av en hybrid kampanje krever et omfattende etterretningsapparat. Bred og hurtig tilgang på etterretninger er nødvendig for trusselaktøren for å søke etter sårbarheter og bygge opp en målliste i forberedelsesfasen, og deretter for å måle effekten av tiltakene i gjennomføringsfasen (Cederberg og Eronen 2015). Denne etterretningsvirksomhet kan i dag gjøres langt mer effektivt, med større utbytte og lavere risiko enn før på grunn av utbredelsen av digitale kommunikasjonsmidler (PST 2016:8)

Strategisk bruk av tvetydighet (*ambiguity*) er det elementet som mer enn noe annet preger staters bruk av hybride virkemidler. Dette er også hovedutfordringen for deteksjon. Hensikten med tvetydighet er å vanskelig- eller umuliggjøre respons, både militært og politisk. Det er et virkemiddel som rettes mot motstanderens beslutningsprosesser (Reichborn-Kjennerud og Cullen 2016:2). Evne til å utnytte oppdukkende muligheter er et sentralt trekk ved russisk strategisk kultur (Covington 2016:4), og Conley og Stefanov (2016:65) registrerer for eksempel stor grad av fleksibilitet i valget av alliansepartnere som benyttes av Russland for politisk påvirkning i Østeuropa.

Trusselaktøren vil forsøke å skape juridisk asymmetri gjennom å maksimere egne muligheter for å operere og samtidig begrense motstanderens handlingsrom. Dette kan oppnås gjennom å holde intensiteten på et så lavt nivå at det ikke utløser en væpnet reaksjon fra forsvareren, eventuelt å begrense seg til å true med væpnet konflikt. Dersom væpnet konflikt bryter ut, vil det være i trusselaktørens interesse å presentere et narrativ om at det er en intern konflikt i mållandet. Det vil trolig være svært vanskelig for forsvareren å tillate allierte styrker å operere på eget territorium dersom det ikke er en anerkjent internasjonal væpnet konflikt (Sari 2016:23). En regjering vil av politiske grunner unngå å innrømme at man har en væpnet konflikt gående med en opposisjonsgruppe for å unngå innblanding fra utenforstående. Regjeringen vil ønske at de

opposisjonelle betraktes som kriminelle, men de opposisjonelle vil ønske anerkjennelse gjennom å fremstå som kombattante som driver lovlige krigshandlinger (Dahl 20008:30).

Cederberg og Eronen (2015) peker på tre viktige trekk ved hybride trusler:

- Identifiserte sårbarheter eller asymmetrier identifiseres og utnyttes systematisk i alle faser, også før en sikkerhetspolitisk krise har oppstått.
- Sårbarhetene utnyttes ved hjelp av overraskelsesmomentet i kombinasjon med fornektbarhet og villedning. For Vestlige stater har det vist seg å være en utfordring å forutsi konflikter og å enes om en strategi, spesielt dersom konflikten er av politisk eller ikke-militær karakter (Hartmann 2017:3).
- Tidsmessig vil trusselaktøren ha mindre fokus på en hurtig og klar "seier", og i stedet eskalere og de-eskalere spenningen, gjerne over lang tid (Hartmann 2017:3, Thiele 2016:6). En pågående trussel som øker og minsker i intensitet er videre med på å utviske grensen mellom krig og fred (Chivvis 2017:2).

I hvilke sammenhenger og med hvilke målsetninger kan vi se for oss at hybride trusler kan komme til anvendelse? Galeotti (2016a:51) har identifisert to tilnærminger for bruk av ikke-lineære, tidvis fordekte, tidvis tvetydige, tidvis åpenbare militære og politiske metoder. Den ene er å legge press på andre stater som et supplement til mer konvensjonell geopolitikk. Den andre tilnærmingen handler om å berede grunnen for en intervensjon. Chivvis (2017:2) tenker i sammen baner når han peker på tre målsetninger som Russland kan tenkes å ville oppnå med hybride metoder: 1) ta territorium uten åpen bruk av militærmakt (som man så på Krym), 2) skape påskudd for militær inngripen (som særlig de baltiske landene frykter), og 3) politisk påvirkning (som er den mest aktuelle trusselen for vestlige land).

Bruk av hybridbegrepet i en statlig kontekst kritiseres først og fremst for at man vanner ut innholdet i begrepet "krig" ved å bruke begrepet "hybridkrig" om alt fra diplomati via propaganda- og mediekampanjer til cyberangrep (Renz og Smith 2016:13, Kofman og Rojanski 2015). Hybridbegrepet kritiseres også for å gjøre det enklere for NATO og Vesten å unngå å reagere på trusselen, siden desinformasjon, økonomisk press, bestikkelser, trusler og «lokale» demonstranter holder seg under terskelen for en Artikkel 5-respons (Schadlow 2015). Kritikken handler også om at begrepet i bunn og grunn ikke inneholder noe nytt. Stater har alltid benyttet

diplomatiske, økonomiske og militære virkemidler for å nå sine mål, og man kan gjerne si at "hybrid krig i en eller annen form like gjerne kan være det normale i konflikter mellom mennesker snarere enn et unntak" (Murray og Mansoor 2012). Men dersom man unnlater å «connect the dots» og knytte de ulike hendelsene man observerer til overordnede politiske målsetninger hos trusselaktøren, vil man ikke få øye på at «krig er en fortsettelse av politikken med andre midler». Det er viktig å huske at hybridbegrepet handler om virkemidlene, ikke om prinsippene eller målsetningene med krigføring (Schadlow 2015).

3.2.2 Beslektede begreper

Litteraturstudien viser at det finnes en rekke beslektede begreper som har fellestrekk med hybridkrig og hybride trusler. Mange av begrepene har blitt til i etterpåklokskapens lys gjennom å analysere vellykkede militære kampanjer (Renz og Smith 2016:3). Tanken om at tidligere suksesser kan kopieres i nye kontekster legger for stor vekt på operasjonelle kapasiteter og for liten vekt på strategi, som alltid vil være kontekstavhengig (*ibid.*). Det er et fellestrekk at debatten rundt disse begrepene i stor grad handler om hvorvidt de representerer noe nytt, og om de tilfører verdi.

Her følger en ikke uttømmende oversikt over en del beslektede begreper:

- Asymmetrical Warfare
    - Svakere aktører som terrorgrupper kan gjennom en asymmetrisk tilnærming vinne over en tallmessig og teknologisk motstander (Renz og Smith 2015:5).
- Counter Insurgency
    - I konflikter med opprørere er ikke teknologisk overtak tilstrekkelig. Kunnskap om lokal kultur og historie og det å vinne over lokalbefolkningens ”hearts and minds” er sentralt (Renz og Smith 2016:5).
- Grey Zone Conflict/Strategy
    - Strategi som typisk benyttes av stater med en revisjonistisk agenda. Omfatter en inkrementell tilnærming over lengre tid, samt koordinert bruk av ukonvensjonelle maktmidler under terskelen for tradisjonell konflikt (Mazarr 2015).

- Indirect action
    - Beskrives som en del av russisk strategisk avskrekkingspolitikk. Målet er å oppnå egne målsetninger ved å sette inn en kombinasjon av militære og ikke-militære, åpne og fordekte virkemidler mot sårbarheter i mållandet og samtidig unngå åpne mellomstatlige konflikter (DIA 2017:41). På samme måte som hybride trusler, benytter russiske kilder begrepet *indirect action* (непрямые действия) for å beskrive amerikansk strategi (Chekinov og Bogdanov 2010).
- Measures short of war
    - Hoffman (2017) kritiserer spesielt gråsonebegrepet for å være for inkluderende, og griper tilbake til Kennans formulering fra 1948 om *"measures short of war"* som en mer passende beskrivelse som understreker at selv om stater benytter illegitime og fordekte maktmidler, så er det ikke snakk om krig. Om Hoffman dermed bidrar til mer klarhet, eller om han kun innfører enda et begrep som er med på å forvirre, er et annet spørsmål som vi lar ligge i denne sammenheng.
- New Generation Warfare/Non-linear Warfare
    - Disse begrepenes anvendelse i forhold til hybride trusler er knyttet til den russiske generalstabssjefen Valeriy Gerasimov og hans artikkel om det moderne trusselbildet, der ikke-militære virkemidler har blitt viktigere enn de tradisjonelle, også omtalt som "Gerasimov-doktrinen" (Karber 2015). Gerasimov selv benytter ikke noen av begrepene (Gerasimov 2013). Russisk militær doktrine bruker begrepet очаговый бой ("arnested-strid") for å beskrive hvordan luftlandestyrker bak fiendens linjer i den første fasen vil operere uavhengig av hverandre i ulike sektorer før en felles "linje" mellom avdelinger etableres (Rodnikovskij 1984). Amerikanske militære kilder omtaler dette som "non-linear warfare" (Grau 1990)[11].

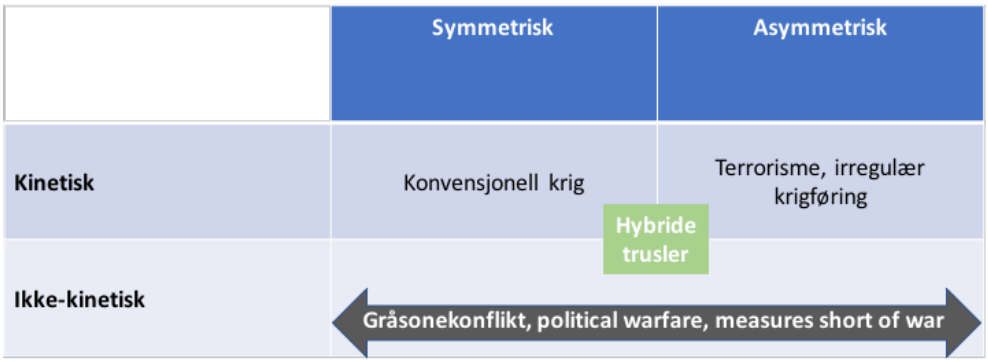
[11] Uttrykket ikke-lineær krigføring (нелинейная война) ble benyttet i en dystopisk novelle skrevet under psevdonym av president Putins rådgiver Vladislav Surkov i mars 2014, et par dager før annekteringen av Krym (Dubovitskiy 2014, Pomerantsev 2014a, 2014b).

- Political Warfare
    - Begrepet overlapper i stor grad med gråsonekonflikter (Mazarr 2015:48). Begrepet knyttes i stor grad til den amerikanske diplomaten George Kennan[12].
    - Kennan trekker linjer til Clausewitz, Marx og Lenin som eksempler på tenkere som erkjenner at krig og fred er et kontinuum, og at krig ikke må isoleres fra sin politiske kontekst (Kennan 1948:1). Begrepet brukes ofte om USA og Sovjetunionens respektive strategier under den Kalde krigen, men har gjenoppstått i dagens diskusjon rundt hybridbegrepet (Galvach et.al.2015), samt i doktrinell form hos amerikanske spesialstyrker (US Army SOC 2015).
- Unconventional Warfare
    - US DoD definerer ukonvensjonell krigføring som krig gjennom en stedfortreder: *" [...] activities to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power through and with an underground, auxiliary, and guerrilla force in a denied area."* (Mazarr 2015:47).
- Unrestricted Warfare/Three Warfares
    - Det første begrepet stammer fra en bok skrevet av to kinesiske offiserer i 1999 (Qiao og Wang 1999) som en reaksjon på den amerikanskledete koalisjonens fremgang i den første Gulfkrigen. "Uinnskrenket krig" omfatter 15 former for "ikke-militære krigsoperasjoner" som en stat kan bruke i kombinasjon for å overvinne en sterkere motstander (Van Messel 2005). *Three Warfares* er People´s Liberation Army sitt godkjente konsept for informasjonsoperasjoner fra 2003,

[12] [Political warfare is] *the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP—the Marshall Plan), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states* (Kennan 1948:1).

bestående av strategiske psykologiske operasjoner, mediemanipulasjon og "legal warfare" (Raska 2015). Konseptet analyseres grundig av Halper (2013).

Til sammenligning kan en hybrid trussel, gitt denne oppgavens brede definisjon, gjøre nytte av ikke-kinetiske virkemidler typisk for "gråsonen", 'political warfare' eller 'measures short of war'. Men samtidig kan en hybrid trussel bestå av militære virkemidler eller gå over i åpen konflikt. Hoffman (2017:6) peker i denne sammenheng på konflikten i Østukraina, som har krevet nesten 10,000 menneskeliv.



Figur 5. Hybride trusler og beslektede begreper plassert i forhold til dimensjonene kinetisk/ikke-kinetisk og symmetrisk/ikke-symmetrisk. Inspirert av Karlsen (2010:28) og Hoffman (2017:3).

Figuren ovenfor er et forsøk på å plassere hybride trusler i relasjon til de andre begrepene som er drøftet. Den illustrerer hvordan en bredt definert hybrid trussel befinner seg på et mellomnivå mellom dimensjonene kinetisk/ikke-kinetisk og symmetrisk/ikke-symmetrisk, i det den kan bestå av ikke-voldelige virkemidler, men også konvensjonelle eller irregulære former for maktbruk.

3.2.3 Delkonklusjon

Hybride trusler er ikke et nytt fenomen, men selve begrepet er en nyttig konstruksjon for å analysere konflikter som involverer ulike dimensjoner som konvensjonell/ukonvensjonell og symmetrisk/asymmetrisk. Det finnes en rekke begreper som beskriver koordinerte og flerdimensjonale trusler, noe som reflekterer tematikkens kompleksitet (Murray og Mansoor 2012). Oppgavens definisjon av hybride trusler er bred i stedet for å dele problemet opp og gi det flere betegnelser som åpner for flere diskusjoner. Definisjonen legger vekt på kombinasjonene åpenlys/fordekt og militær/ikke-militær, koordinasjon i tid og i ulike dimensjoner, samt

minimering av politisk risiko. Av den forutgående drøftingen kan man utlede flere momenter som vanskeliggjør deteksjon av en koordinert hybrid trussel:

- Dersom aktiviteten er stadig pågående over lang tid, vil forsvareren gradvis venne seg til å leve med trusselnivået. Etterretningsvirksomhet, informasjonsoperasjoner og cyberangrep er eksempler på aktivitet som pågår både i fred, krise og krig. Situasjonen vil ligne en "krypende krise" i t'Hart og Boins typologi som ble presentert i kapittel 3.
- Autoritære stater har langt større muligheter til å prioritere og koordinere sine tiltak på tvers av sektorer, mens liberale demokratier, deriblant Norge, preges av at ansvar for sikkerhet er spredt over mange sektorer. *Failure of foresight*-modellen og HRO studier som ble presentert i kapittel tre peker blant annet på utfordringer med informasjonshåndtering i komplekse systemer. *Stakeholder involvement*-modellen viser behovet for bred involvering for å håndtere komplekse risikoer.
- Tvetydighet oppnås gjennom metoder som umerkede militære styrker, stedfortredere, cyberangrep og trekk ved modus operandi som bruk av overraskelsesmomentet, opportunisme, avledning og politisk *deniability*. Tvetydighet vanskeliggjør deteksjon spesielt og beslutningsprosessen generelt. Attribusjon av trusselen er sentralt, og kan forbedres ved kartlegging av sårbarheter, som igjen støtter trusselvurderingene (intensjon og kapabilitet) som utarbeides gjennom etterretning.
- Påvirkningsoperasjoner peker "de utenforståendes" betydning i *Stakeholder involvement*-modellen. Her representert ved grupper i befolkningen som kan la seg påvirke.

4. Resultater/empiri

4.1 Morfologisk analyse

Problemstillingen for den morfologiske analysen er å beskrive hvilke metoder, virkemidler og verktøy en statlig trusselaktør kan tenkes å benytte i en hybrid kampanje.

4.1.1 Parametere og parameterverdier

Hybridbegrepet har blitt benyttet om ulike typer konflikter og om ulike typer trusselaktører, både statlige og ikke-statlige, noe som har bidratt til å gjøre begrepet utydelig. De sentrale aspektene ved hybride trusler er hvilke kapabiliteter og sårbarheter de involverte aktørene har, samt hvilke midler som blir benyttet for å oppnå hvilke effekter (Reichborn-Kjennerud og Cullen 2016:2).

Analysen vil derfor ikke inneholde aktør som en parameter, men vurdere hvordan tilgjengelige metoder (strategier) kan gjennomføres med ulike virkemidler (handlinger) støttet av konkrete verktøy (kapabiliteter).

Det er statlige trusselaktører som er fokus for scenarioene og analysen, og det er staten Norge som er trusselens referanseobjekt. Montevideokonvensjonen fra 1933 fastslår følgende fire kriterier for hva som definerer en stat (Vandepeer 2011:57): en permanent befolkning, et definert territorium, en regjering samt mulighet til å ha relasjoner til andre stater. Disse kriteriene utgjør da fire aspekter ved en stat som kan bli utsatt for en trussel: befolkning, territorium, styresett og interesser. Det ville vært interessant å inkludere parametere som beskriver referanseobjektet (Norge) i analysen, men omfanget gjorde ikke dette mulig.

Parameteren mål (trusselaktørens ambisjoner og målsettinger) har vært forsøkt i ulike varianter, men til slutt blitt forkastet, da den ikke tilfører analysen verdi. Blant annet ble følgende kombinasjon forsøkt: Ta kontroll over territorium uten åpen militærmakt; nekte bruk av territorium eller domene; påvirkning. Kombinasjonen ble forkastet, siden det viste seg at parameteren påvirkning var konsistent med de fleste løsninger, noe som ga et alt for bredt utgangspunkt for det videre arbeidet.

Utgangspunktet for analysen er derfor at målsetningen for å bruke hybride metoder ikke skiller seg fra andre situasjoner der stater bruker vold eller fordekte metoder for å nå sine mål. Arnold Wolfers (1962:91) deler staters utenrikspolitiske mål i tre generelle kategorier: self-extension (endring i status quo), self-preservation (bevare status quo), self abnegation (”altruistiske” mål som internasjonal solidaritet, legalitet, rettferdighet, humanitære saker). Når Clausewitz hevder at ”krig er en fortsettelse av politikken med andre midler”, impliserer dette at det finnes et gitt punkt der politikken stanser, og militær konflikt starter. Denne grensen gjelder ikke for hybrid krig (Dayspring 2015:14). Målene med konflikten er fremdeles politiske, men bruken av maktmidler er ikke begrenset til åpen konvensjonell krig. Slik blir ”diplomati en fortsettelse av krigen med andre midler” (Zhou Enlai i Feaver 2010).

Metode

Med metoder forstås trusselaktørens strategi for å oppnå ønsket effekt. Strategi brukes her som en overordnet plan for handling (Johansen 2014:13).

Metodevalget styres ut fra hva man ønsker å oppnå og hvilke ressurser som er tilgjengelige. Det finnes ikke nye spesielle kapabiliteter eller teknologier øremerket for hybridkrig, det er snarere koordineringen av metoder og muligheten for å la en metode ta over for en annen som er det sentrale (Dayspring 2015:14). Muligheten til å la en metode substituere for en annen, for eksempel ved at man svekker motstandsviljen gjennom økonomisk press i stedet for å true med militære virkemidler, vanskeliggjør deteksjon og varsling ved at attribusjon av enkelthendelser blir mer komplisert, og ved at antallet potensielle mål utvides (Ciluffo og Clark 2012:49). For metodeparameteren er det valgt å dele inn i militære, utenrikspolitiske, informasjonsmessige og fordekte metoder. I flere sammenhenger er også juridiske metoder (*lawfare*) definert som en egen kategori[13] under metoden utenrikspolitikk, siden det handler om å (mis)bruke folkeretten eller rettsvesenet for å oppnå politiske målsetninger. Verdiene som brukes i analysen er dermed militært, utenrikspolitisk, informasjon, økonomisk og fordekt.

Militært

Med militært menes et lands væpnede styrker (land, sjø, luft, kjernefysisk, spesialstyrker, cyber). Spesialstyrker kan i enkelte sammenhenger operere fordekt (Bukkvoll 2016:27). Militære styrker vil ellers stort sett operere åpent i den forstand at de kan identifiseres med det land de tilhører, og offensiv bruk av dem kan derfor lede til motangrep, internasjonale sanksjoner eller andre straffetiltak (Dayspring 2015:28).

13

Moore (2017:39) definerer lawfare som en del av informasjonsoperasjoner, og man kan for så vidt også se for seg lawfare som en del av økonomisk påvirkning.

Utenrikspolitisk

Utenrikspolitikk defineres her som "territorialstatens utad- og formålsrettede virksomhet der strategier velges og virkemidler anvendes i lys av statens kollektive selvforståelse (identitet), utenrikspolitiske målsetninger, maktmidler [...] og de konkrete utfordringene staten står overfor" (Fermann 2010:70). Juridiske metoder i vår sammenheng omtales gjerne som *legal warfare* eller *lawfare*, og omfatter utnyttelse av det juridiske systemet for å oppnå operasjonelle målsetninger i stedet for gjennom tradisjonelle militære virkemidler (Moore 2017:40, Bachman og Mosquera 2017:66).

Informasjonsoperasjoner

I en hybrid konflikt spiller befolkningens persepsjon en sentral rolle. Krigspropaganda har eksistert til alle tider, men moderne kommunikasjonssystemer øker mulighetene for å påvirke befolkningens persepsjon i alle faser av en konflikt. For å "vinne krigen" er det ikke tilstrekkelig å nedkjempe motstanderens styrker. Både egen befolkning, befolkningen i konfliktområdet og den internasjonale opinionen må også *tro* at krigen er over, slik at suksess på slagmarken får et tilsvarende politisk resultat (Murray 2012:9). Informasjonsoperasjoner (IO) kan defineres som *«[…] muligheten, gjennom endring, påvirkning og bruk av informasjon, informasjonssystemer og informasjonsprosesser, til å angripe og påvirke en eller flere motparter, beskytte egne styrker og beslutningstakere, samt informere og engasjere tredjeparter»* (Hagen og Søgaard 2014:7). Hensikten vil være å forvirre en befolkning gjennom å skape tvil om hva som er sant (Chivvis 2017:5). IO er en konstant, pågående aktivitet for å sikre langsiktig innflytelse på oppfatninger og holdninger (Cheng 2012:3).

Økonomisk

I en utenrikspolitisk kontekst er incentiver (bistand), tollbarrierer, boikott, beslag og blokader ulike former for maktbruk (Fermann 2010:66). Den økonomiske maktbruken kan være direkte og indirekte. Den kan også være både lovlig og ulovlig. Direkte maktbruk kan være å stenge energileveranser som et forhandlingstrekk. Russlands bruk av infrastruktur i form av gassrørledninger til å dominere både politikk og økonomi i flere land i Østeuropa er et eksempel på indirekte maktbruk. Selv om dette er snakk om lovlig virksomhet, vil måten denne innflytelsen brukes på være problematisk (Chivvis 2017:4). Korrupsjon er et eksempel på ulovlig økonomisk maktbruk.

Fordekt

Fordekte eller klandestine metoder (covert action)[14] omfatter bruk av etterretningstjenester eller spesialstyrker til å bestikke, utpresse og på andre måter påvirke det politiske systemet i et annet land (Chivvis 2017:4). Herman (1996:55) omtaler covert action som en av etterretningstjenesters «sideaktiviteter»[15]. Covert action inkluderer ifølge Herman påvirkningsagenter, skjult politisk finansiering, forfalskning, mediaoperasjoner og «svart» propaganda i den «myke enden», og fordekt støtte til opposisjons- og opprørsgrupper, sabotasje og paramilitære operasjoner i den «harde enden». I denne analysen er imidlertid propaganda plassert under metoden informasjonsoperasjoner for å fremheve betydningen av tiltak i det kognitive domenet. I det digitale rom vil digitale angrep (CNA – *computer network attack*) i den hensikt å ødelegge digital eller fysisk infrastruktur kunne karakteriseres som del av fordekt metode, til forskjell fra digital spionasje (CNE – *computer network exploitation*) som handler om informasjonsinnhenting (Lowenthal 2015:356, Clark 2013:140).

Virkemiddel

Parameteren virkemiddel representerer handlinger som er nødvendig for å gjennomføre en gitt metode. Virkemidlene kan være mer eller mindre krevende å gjennomføre, de kan være åpne eller fordekte, og de kan ha lav eller høy intensitet (grad av voldsbruk).

Militær operasjon

Militære operasjoner kan i denne sammenhengen være offensive eller defensive. En offensiv militær operasjon innebærer bruk av omfattende militær makt, vanligvis i alle domener (land,

[14] I russisk sammenheng omtales denne praksisen som ”aktive tiltak” (активные мероприятия): "*Agent-operational measures aimed at exerting useful influence on aspects of the political life of a target country which are of interest, its foreign policy, the solution of international problems, misleading the adversary, undermining and weakening his positions, the disruption of his hostile plans, and the achievement of other aims”* (Mitrokhin 2013). Til forskjell fra vestlige etterretningstjenester var covert action ikke en sideaktivitet, men en helt sentral oppgave for sovjetisk etterretning (Herman 1996:54). KGB aktive tiltak strakte seg fra manipulering av media til ulike grader av voldsbruk (Andrews og Mitrokhin 1999:224). Denne virksomheten ser ikke ut til å ha avtatt etter 1991, men snarere blitt forsterket ved hjelp av digital spionasje som med relativt liten risiko fremskaffer informasjon som kan lekkes for å påvirke en motstander (Kragh og Åsberg 2017, Rid 2017, Galeotti 2017).

[15] Andre «sideaktiviteter» som nevnes av Herman (2016:55) er kontraetterretning, informasjonssikkerhet, fordekt diplomati, villedning og elektronisk krigføring.

luft, sjø, cyber) for å slå ut en motstander, mens en defensiv militær operasjon har som mål å etablere et forsvar mot angrep fra en annen aktør og hindre denne i å realisere sine mål (Johansen 2014:13).

Militært press

Militært press innebærer trusler om maktbruk gjennom for eksempel deployeringer, beredskapsheving, (ikke-varslede) øvelser, overflygninger og andre former for grensekrenkelser eller avfyring av varselskudd (Johansen 2014:13, Karber 2015).

Multilateralt diplomati

Internasjonale organisasjoner eller multilateralt diplomati kan være et virkemiddel dersom en stat bruker dem på en illegitim måte til sin revisjonistiske agenda (Mazarr 2015:24). Multilateralt diplomati inkluderer også track-2 diplomati (Mazarr 2015:24), der stater deltar i eller tilbyr å være vertskap for standard-settende organer eller track-2 prosesser for å fremme sin egen agenda på en illegitim måte[16].

Bilateralt (tvangs)diplomati

Bilaterale forhandlinger kan spenne fra presentasjon av argumenter for å overbevise den andre siden, via belønninger og innrømmelser til trusler om militære reaksjoner (Eschevarria (2016:35). Mer subtile former for bilateral påvirkning kan også forekomme[17]. En småstat som Norge søker gjerne multilaterale arenaer fremfor direkte forhandlinger med stormakter [18] (Fermann 2010:61).

---

[16] Den estiske sikkerhetstjenesten beskriver hvordan estiske organisasjoner som Legal Information Centre for Human Rights og Russian School in Estonia ble finansiert av russiske myndigheter for å delta i OSCEs årlige Human Dimension Implementation Meeting for å fremsette uriktige påstander om Estland (Kapo 2016:7). En annen form for misbruk av internasjonale organisasjoner kan være fremsettelse av politisk motiverte arrestordre gjennom Interpol (Townsend 2017).

[17] Utdeling av pass i etniske enklaver, støttet av justering av egen statsborgerlov er en metode som Russland har benyttet i Abkhasia, Sør-Ossetia, på Krym og i Østukraina (Grigas 2016, Orekh'' 2008). Basert på FN-prinsippet om "responsibility to protect" skaper man dermed påskudd for å gripe inn for å beskytte egne statsborgere på et annet lands territorium.

[18] Regjeringens linje for reaksjoner mot Russland etter folkerettsbruddene i Ukraina i 2014 var at norsk sikkerhet forvaltes best gjennom internasjonalt samarbeid ved at landet sluttet seg til EUs og nære alliertes reaksjoner fremfor å stå alene, noe som ville vært et dramatisk brudd med norsk sikkerhetspolitikk siden 1945 (Røsland 2017).

Støtte politiske, interessegrupper

Russisk støtte til politiske grupper eller andre former for interessegrupper er kjent fra flere europeiske land. I mange tilfeller har høyreekstreme grupper som tidligere fokuserte på etniske, religiøse og seksuelle minoriteter som "fiender" rettet sin oppmerksomhet mot geopolitiske spørsmål (Krekó et. al. 2017:9). Relasjonen mellom trusselaktør og stedfortreder kan være ideologisk eller en form for transaksjon (i form av varer eller tjenester). Relasjonen kan være ad hoc eller en langvarig allianse (Ciluffo og Clark 2012:49).

Etablere de facto tilstedeværelse (ikke-mil)

Ikke-militære ressurser som kystvakt, fiskefartøyer, NGOer og næringsliv kan brukes for å etablere en de facto tilstedeværelse i omstridte områder som del av en langsiktig kampanje (Mazarr 2015:59).

Public diplomacy

Public diplomacy betegner en internasjonal aktørs forsøk på å påvirke det internasjonale miljøet gjennom å engasjere et utenlandsk publikum (Kragh og Åsberg 2017). Begrepet oppstod på 1960-tallet som et forsøk på å distansere staters informasjonsaktiviteter fra det mer belastende propaganda-begrepet[19]. Public diplomacy kan inkludere utvekslingsprogrammer for studenter, språkopplæring, kulturaktiviteter og kringkasting. Ved siden av bilateralt stat-til-stat og multilateralt diplomati er public diplomacy en kanal som benyttes av ikke-statlige aktører som internasjonale organisasjoner, NGOer og næringsliv (USC u.å).

Propagandaoperasjon

Propagandaoperasjoner kan være "hvite" og ha en tydelig avsender, eller de kan være fordekt ("grå" eller "svarte") i ulik grad (Kofman 2016, Snow 2017:399). Desinformasjon regnes som en form for propaganda.

Sanksjoner

Økonomiske sanksjoner og embargo er straffetiltak benyttes for å påvirke andre stater til å handle på en bestemt måte (Öhme 2017). Sanksjoner kan ta form av reiseforbud, "frysing" av kapital, ekspropriering, reduksjoner i økonomisk assistanse eller handelsrestriksjoner (Allen & Overy 2014:2, Jackson 2015:11). Sanksjoner kan være vidtrekkende og forby all kommersiell virksomhet med et annet land (USAs embargo mot Cuba), eller de kan være målrettede, for eksempel mot enkelte varer, aktører eller enkeltpersoner (Masters 2017).

[19] Mens public diplomacy er rettet mot publikum i andre stater, benyttes på engelsk begrepet public affairs om en stats kommunikasjon med sin egen befolkning (uscpublicdiplomacy.org).

Korrupsjon

Den estiske sikkerhetstjenesten slår fast at korrupsjon kan utgjøre en ekstern sikkerhetstrussel i de tilfeller der andre stater forsøker å påvirke myndighetenes beslutninger gjennom utpressing av individer eller grupper (Kapo 2016:34).

Implisert økonomisk tvang

Investeringer og oppkjøp (foreign direct investment) av bedrifter i et land man ønsker å påvirke kan være legitime eller del av korrupsjon (Öhme 2017). Kontroll over infrastruktur som gassledninger vil skape en monopolsituasjon som kan brukes som et politisk pressmiddel overfor andre (Chivvis 2017:4).

Manipulere folkeretten

Folkeretten er rettsregler som primært gjelder forholdet mellom stater[20]. Folkeretten skiller seg fra nasjonal rett ved at det mangler sentral lovgivningsmyndighet og håndhevingsorganer. Praktisering av folkeretten er dermed for en stor del overlatt til statenes respekt for avtaler de har inngått (Dahl 2008:23). De viktigste rettskildene er sedvanerett, traktater og dommer (*ibid.*:24). For å oppnå bred tilslutning til traktater har det ofte vært nødvendig å benytte tvetydige formuleringer som er åpne for tolkning (*ibid.*:27).

Utforming av lover

Nasjonale lover som Kinas *Law on Territorial Sea and Contiguous Zone* kan benyttes for å underbygge territorielle krav mot andre land (Halper 2013:62-63). På samme måte oppgraderte Kina i 2012 kystlandsbyen Sansha til byprefektur i Hainanprovinsen, for å støtte kravene om råderett over omstridte øyer i Sørkinahavet (*ibid.*:67). Russland har utformet en rekke lover nasjonalt for å underbygge intervensjon i andre land, blant annet anneksjonen av Krym (Prezident Rossii 2014) og endringer i loven om statsborgerskap for at russisk-talende personer i utlandet enklere kan få russisk statsborgerskap (Zatulin 2016, Bratersky 2012).

[20] Kina benytter jevnlig manipulering av United Nations Convention on the Law of the Sea (UNCLOS) som et virkemiddel for å sikre sitt fotfeste i Sørkinahavet, både ved å underminere andre staters juridiske krav og ved å etablere argumenter for Kinas posisjoner i internasjonal rettspraksis gjennom å etablere fait accompli gjennom å bygge opp kunstige øyer og deretter gjøre krav på territorialfarvann og eksklusive økonomiske soner rundt dem (Jackson 2015:6). President Putins henvisning til internasjonal humanitær rett for å rettferdiggjøre intervensjon i Ukraina er et annet eksempel på måter internasjonal rett kan utnyttes (Buckley og Pascu 2015).

Rettsforfølge nasjonalt

Politiserte dommer mot enkeltpersoner er et annet eksempel på bruk av legale virkemidler for å sende et politisk budskap og skape falsk legitimitet. Det finnes en rekke eksempler på rettsforfølging av for eksempel ukrainske enkeltpersoner i Russland, både ved at de har blitt arrestert, men også *in absentia* (Voyger 2015).

Fordekte operasjoner

Fordekte operasjoner omfatter etterretningsinnhenting og covert action. Etterretningsinnhenting (menneskelig eller teknisk) er en aktivitet som pågår i alle faser av en konflikt og som støtter aktive tiltak, enten fordekte eller militære operasjoner (Mazarr 2015:59). Covert action kan ta form av trusler, utpressing, sabotasje både i det fysiske og i det digitale rom (Chivvis 2017:4).

Vold v/stedfortreder

Demonstrasjoner, opprør, terrorangrep, attentat og fysisk sabotasje er eksempler på voldelige aksjoner som kan iverksettes ved hjelp av stedfortredergrupper (Chivvis 2017:4). Hvilken tilnærming som benyttes vil avhenge av hvilke sårbarheter i mållandet trusselaktøren ønsker å utnytte (Ciluffo og Clark 2012:49).

Cyberangrep

NATO definerer cyberangrep som "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself" (CCDCOE u.å.). Andre definisjoner inkluderer også fysisk skade på for eksempel industrielle systemer ved hjelp av cyberangrep (*ibid.*). Det er vanskelig å etablere en klar forskjell i alvorlighetsgrad mellom fysisk sabotasje og cyberangrep. Man kan åpenbart se for seg cyberangrep som er så omfattende at de kan likestilles med et militært angrep. NATO har besluttet at alvorlige cyberangrep kan utløse en artikkel 5-respons fra alliansen (Oliphant og McGoogan 2017, FD 2016:35).

Verktøy

Parameteren verktøy omfatter materielle kapasiteter som er nødvendig for å gjennomføre et virkemiddel.

Kjernefysiske styrker

Trusler om bruk av kjernefysiske styrker for å forsvare sine vitale interesser tjener til å understreke faren ved eskalering av en konflikt der hybride metoder inngår (Mazarr 2015:61).

Spesialstyrker

Spesialstyrker er trent til å operere selvstendig bak fiendens linjer og kan utføre en rekke oppgaver. De kan brukes til å lære opp, bevæpne eller liaisonere med lokale opprørere. Under annekteringen av Krym benyttet Russland spesialstyrker uten nasjonale kjennetegn for å bidra til forvirring og forsinke beslutningsprosessen på ukrainsk side. Selv om spesialstyrker er en del av det militære apparatet kan de benyttes på ukonvensjonelle måter, for eksempel for å oppnå politiske mål uten maktbruk (Bukkvoll 2016:27).

Konvensjonelle styrker

Konvensjonelle styrker (land-, luft-, sjø- og i økende grad cyberdomenet) kjennetegnes ved at de har stor mobilitet og ildkraft og er trent for tradisjonell høyintensiv krig. De vil ofte operere i fellesoperasjoner. Konvensjonelle styrker er store organisasjoner med et omfattende kommando- og kontrollapparat, noe som kan gjøre dem mindre fleksible (Karlsen 2010:31). Ved siden av kinetiske kapabiliteter vil militære operasjoner være støttet av elektronisk krigføring (EK), eller aktiv bruk av det elektromagnetiske spektrum i krigføring for å jamme for eksempel kommando- og kontrollsystemer, radar og GPS-signaler (Ravndal 2016:38). I en mer holistisk russisk tilnærming er EK (радиоэлектронная борьба/РЭБ - radioelektronisk strid) i dag et svært vidt begrep som omfatter elektroniske støttetiltak (teknisk etterretning), angrep (inkludert psykologiske operasjoner[21] og datanettverksangrep) og egenbeskyttelse (Defence Intelligence Agency 2017:42, McDermott 2017:4).

[21] Vestlige styrker har i liten grad trengt å ta hensyn til EK de siste tiårene. Erfaringer fra Ukraina tilsier imidlertid at det er nødvendig å trene på å operere under forhold med utstrakt bruk av EK og cyberangrep, inkludert bortfall av GPS-signaler (Giles 2016:57). I konflikten i Donbass skal det ifølge ukrainske kilder også ha forekommet både masseutsendte og målrettede falske sms-meldinger til militært personell og deres pårørende (Ak-Murza 2014, Gusarov 2016).

Organisert kriminalitet

Organiserte kriminelle kan benyttes som stedfortreder for å utøve innflytelse på individer eller myndigheter (Radin 2017:20, Galeotti 2016a:72). Aktiviteten kan dreie seg om smugling, narkotika, trafficking og utpressing (Hoffman 2010:3). Smuglernettverk kan benyttes både til å frakte materiell over grenser, kartlegging av grensevaktens personell og til å delta i fordekte operasjoner (Kapo 2016:15, VSD 2016:27).

Stedfortredere

Stedfortredere er ikke-statlige tredjeparter, for eksempel politiske grupper, andre interessegrupper eller kriminelle (Radin 2017:6). Grupper som sympatiserer med et lands agenda kan representere slike stedfortredere (Chivvis 2017:4)[22], men relasjonen kan også være av mer transaksjonsmessig natur (Ciluffo og Clark 2012:49).

Etterretningstjeneste

Etterretning handler primært om å samle inn informasjon ved hjelp av tekniske eller menneskelige kilder for å gi oppdragsgiveren et bedre beslutningsgrunnlag. Etterretningstjenester kan også bruke aktive metoder (covert action), enten voldelig eller gjennom påvirkning. I sin trusselvurdering slår PST (2017:8) fast at flere land også benytter etterretningsvirksomhet til å gi sin egen industri konkurransefordeler. Her er etterretning begrenset til å kun omfatte statlige etterretningsorganisasjoner, og ikke etterretningsvirksomhet som også kan drives av nettverk eller selskaper/foretak i form av industrispionasje.

Diplomati

Diplomati kan brukes til å fremme aggressorstatens interesser i internasjonale organisasjoner eller i bilaterale settinger ved hjelp av forhandlinger, påtrykk og direkte utpressing. Aktiviteten kan rettes direkte mot landet man ønsker å påvirke eller mot en bredere internasjonal opinion (Öhme 2017). Målsetningen kan for eksempel være å sverte omdømmet til eller å isolere landet som er utsatt for en hybrid trussel gjennom å svekke internasjonalt samhold.

[22] Eksempler på russisk bruk av politiske stedfortredere er "diskusjonsklubber" for russisktalende i baltiske land (Kapo 2016:10) og støtte til anti EU-grupper i Nederland og anti skifergassgrupper i Bulgaria (Radin 2017:4). En russisk gruppe som ligger i grenselandet mellom politisk og voldelig stedfortreder er den nasjonalistiske russiske motorsykkelklubben "Night Wolves", som har blitt brukt som rekrutteringsbase for operasjoner i Donbass, og som oppfattes som en sikkerhetstrussel av sentraleuropeiske og baltiske land (Galeotti 2016:297).

Redigerte medier

Redigerte medier har en sentral redaktørfunksjon og oppfattes gjerne som mer troverdige. I en norsk kontekst forholder redigerte medier seg som regel til pressens eget regelverk gjennom for eksempel Vær Varsom-plakaten og Redaktørplakaten. Nettsteder som Wikipedia er også i en viss forstand "redaktørstyrte" gjennom at artikler uten kildehenvisninger merkes som mangelfulle av bidragsytere. Avisenes kommentarfelter befinner seg i en gråsone mellom redigerte og ikke-redigerte medier (Høgskolen i Bergen 2015). Russland benytter statsfinansierte "uavhengige" medier som RT og Sputnik for å formidle Kreml-vennlige narrativer og for å spre falske eller forvirrende budskap.

Uredigerte medier

Wikipedia.no definerer sosiale medier som: "[...] medier (kanaler eller plattformer) som ved hjelp av Internett eller web-basert teknologi, åpner for interaksjon mellom to eller flere mennesker (brukere). [...] I motsetning til tradisjonelle medier (TV, avis, radio) er det brukerne som setter føringen for hva innholdet skal være, og ikke en overordnet aktør/avsender".

Næringsliv

Gjennomføring av en hybrid kampanje forutsetter at staten er i stand til å koordinere både militær og sivil sektor, noe som også kan innbefatte næringslivet. Bruk av kinesiske fiskebåter i Sørkinahavet som en "maritim milits" er et eksempel på at næringslivet kan fungere som en styrkemultiplikator som skaper et uklart bilde av situasjonen i området (Jackson 2015:11, Mazarr 2015:86). Et annet eksempel er Kinas utplassering av oljeplattformen HYSY 981 i vietnamesisk økonomisk sone (Murphy 2012, Jackson 2015:10). Andre typer organisasjoner, som for eksempel NGOer og forskningsinstitusjoner kan tenkes brukt på liknende måter[23].

[23] Den russisk-ortodokse kirken brukes som et politisk instrument for å knytte tettere bånd til kirkesamfunn i andre ortodokse land som Serbia og Bulgaria (Conley og Stefanov 2016:6).

Rettsvesen

Et politisert rettsvesen kan benyttes som et verktøy for å oppnå strategiske målsetninger. I følge russisk lov har rettsvesenet en selvstendig stilling, men dommere er like vel utsatt for påvirkning fra utøvende myndigheter, militære og sikkerhetstjenestene. Spesielt i høyprofilerte eller politisk sensitive saker er utfallet gjerne gitt på forhånd (U.S. Department of State 2016). For utenlandske investorer medfører dette at man i liten grad har rettslige garantier for sine investeringer, og dermed kan rettsvesenet også benyttes som del av tiltak på det økonomiske området (Hagen 2009, Forskningsrådet 2006).

Hackergrupper

Hackergrupper ligner stedfortredere på den måten at de handler på vegne av aggressor-staten på fordekt vis, men i det digitale domenet. Hackergruppene kan ha ulike grader av tilknytning til en stat, i form av for eksempel finansiering og kommando & kontroll. De kan være ideologisk motivert, eller drevet av egne økonomiske motiver. Bruk av hackergrupper til å utføre cyberangrep gjør attribusjon mer komplisert, og øker muligheten for at trusselaktøren kan holde seg skjult (Saalman 2017:3).

4.1.2 Morfologisk rom

Tabellen under oppsummerer parametere og parameterverdier som er anvendt i analysen.

Metode	**Verktøy**	**Virkemiddel**
militært	kjernefysiske styrker	offensiv mil operasjon
politisk	spesialstyrker	militært press
informasjon	konvensjonelle styrker	multilateralt diplomati
økonomisk	organisert kriminalitet	bilateralt (tvangs)diplomati
fordekt	stedfortredergrupper	støtte stedfortredergrupper
	etterretningstjeneste	etablere de facto tilstedeværelse
	diplomati	public diplomacy
	redigerte medier	propagandaoperasjon
	sosiale medier	sanksjoner
	NGO	korrupsjon
	næringsliv	implisert økonomisk tvang
	rettsvesen	manipulere internasjonal rett
	hackergrupper	utforming av lover
		rettsforfølge nasjonalt
		fordekte operasjoner
		vold v/stedfortreder
		cyberangrep

4.1.3 Syntesefase

Det foregående avsnittet representerer det forfatteren teoretisk oppfatter som mulige kombinasjoner av metoder, virkemidler og verktøy som en statlig trusselaktør kan tenkes å benytte i en hybrid operasjon. Neste fase i analysen er å avdekke hvilke løsninger som er konsistente (kan opptre sammen) og deretter klassifisere løsningene i scenarioklasser. Syntesefasen innebærer en systematisk gjennomgang av alle mulige kombinasjoner (kan X og Y opptre samtidig?). Det vil bli for omfattende å presentere alle vurderingene som er gjort her, men kun de mest signifikante vurderingene som er gjort for de ulike metodene i matrisen. En viktig observasjon i syntesefasen er betydningen av det digitale domenet for mange av de identifiserte metodene. Militære operasjoner, informasjonsoperasjoner i ulike varianter og ulike former for fordekt virksomhet er alle avhengige av moderne kommunikasjon for rekognosering, planlegging, gjennomføring og vurdering av effektene. Dermed er kontroll over aktivitet i det digitale domenet viktig for deteksjon av trusler.

Militært

Den militære metoden kan i vår sammenheng benyttes til enten å gjennomføre offensive eller defensive operasjoner, samt til å utøve press eller avskrekking. Et kjernefysisk angrep er satt som inkonsistent med hybride operasjoner, men kjernevåpen vil naturlig nok ha en rolle i å utøve press eller avskrekking mot andre stater. I tillegg til å operere i de tradisjonelle domenene land, sjø og luft støttet av elektronisk krigføring, kan konvensjonelle styrker også gjennomføre angrep i det digitale rom ved siden av etterretningstjenester og stedfortredere som hackergrupper eller kriminelle. Spesialstyrker kan i tillegg til å delta i militære operasjoner sammen med andre våpengrener også operere fordekt. Eksempler fra Krym i 2014 viser at også konvensjonelle styrker kan opptre uten kjennemerker, men for analysen er denne operasjonsformen definert som en spesialoperasjon.

Politisk

Den utenrikspolitiske metoden kommer stort sett til uttrykk gjennom at man bruker diplomati, enten bi- eller multilateralt for å øve press mot andre stater. Støtte til stedfortredergrupper i et annet land kan i tillegg foregå ved hjelp av NGOer, næringsliv eller etterretningstjenester.

Finansiell støtte til en politisk bevegelse i et annet land kan for eksempel kanaliseres gjennom NGOer eller næringslivsaktører. I de tilfeller der en stedfortredergruppe ikke lenger opptrer kun som en ikke-voldelig politisk bevegelse, men begynner å benytte voldelige midler, vil støtten skje ved gjennom en mer fordekt tilnærming. Etterretningstjenester vil dermed være mer sentrale enn diplomati. Public diplomacy er i vår analyse plassert som et politisk virkemiddel, og ikke under informasjonsoperasjoner. Dette reflekterer at public diplomacy er mer eller mindre direkte kommunikasjon rettet mot befolkningen i en annen stat. Public diplomacy kan utøves gjennom uttalelser fra politisk ledelse eller gjennom ambassader, for eksempel gjennom "åpne brev" til et annet lands befolkning (Den russiske ambassade Oslo 2017 a, b, c). Juridiske virkemidler er som tidligere nevnt i vår sammenheng sortert under utenrikspolitisk metode. Vurderingen som ligger bak er at manipulering av internasjonal rett, utforming av lover som diskriminerer personer eller bedrifter fra et bestemt land eller rettsforfølging av disse først og fremst vil være politisk styrt.

Informasjonsoperasjoner

Informasjonsoperasjoner består i analysen av parameteren propaganda. Dette er en pågående aktivitet i alle faser av en konflikt. Propagandaen kan være åpen, og vil da ligge nært opp til det vi har definert som public diplomacy. Såkalt «svart» propaganda vil derimot være fordekt på den måten at den egentlige avsenderen er skjult. Desinformasjon handler om å villede mottageren av budskapet ved å sende ut direkte falsk informasjon, eller informasjon som er sterkt ensrettet eller subjektiv. Informasjonsoperasjoner kan både rettes mot et hjemmepublikum, eller mot befolkningen i andre stater. Begge virkemidler kan utføres gjennom et bredt spekter av verktøy (stedfortredergrupper, etterretningstjenester, diplomati, redigerte medier, sosiale medier, hackergrupper). I en autoritær stat vil redigerte media (tv, radio, aviser) i større eller mindre grad være kontrollert av regimet, og vil dermed først og fremst fungere som et talerør for disse.

Økonomisk

Økonomiske virkemidler kan i analysen utføres gjennom henholdsvis diplomati eller næringsliv. Implisert økonomisk tvang kan som nevnt tidligere utøves gjennom at eiendom eller bedrifter blir kjøpt opp av representanter for en annen stat, eller ved at det etableres infrastruktur som «mållandet» er avhengig av å bruke. Dette er i utgangspunktet lovlig virksomhet, men som like vel kan brukes som et politisk pressmiddel i en gitt situasjon. Korrupsjon befinner seg i den ulovlige enden av skalaen. Dette kan være et aktuelt pressmiddel som iverksettes for å legge

press på enkeltpersoner. Implisert økonomisk tvang kan dermed også utføres gjennom et bredere spekter av virkemidler (organisert kriminalitet, diplomati og næringsliv), noe som kan være med på å skape tvetydighet og gjøre det mer utfordrende å forstå at man er utsatt for en koordinert trussel.

Fordekt

De fordekte virkemidlene kan gjennomføres med en rekke verktøy, noe som (i tillegg til at de nettopp er fordekte) skaper vanskeligheter for deteksjon og attribusjon av trusselen. Virkemiddelet etterretningsinnsamling kan i denne analysen kun utføres av etterretningstjenester. Det ligger imidlertid i sakens natur at de konkrete aktørene som utfører etterretningsinnsamling i mange tilfeller vil fremstå som noe annet (diplomater, NGOer, næringslivsaktører, forskere etc.). Fordekte operasjoner (covert action) er tiltak som trusler, utpressing, sabotasje osv. som foregår i det fysiske domenet, mens cyberangrep (CNA) er sabotasje i det digitale domenet.

4.1.4 Løsningsrom

Tabellen under viser de mulige løsningene som er resultatet av konsistensanalysen, og som kan brukes videre for å bygge scenarioer. I kapittel 2 ble krav følgende krav til typologien satt: i) praktisk brukbar, ii) realistisk, iii) forståelig, iv) godt begrunnet, v) dekkende eller uttømmende og vi) gjensidig utelukkende. Typologien anses som praktisk brukbar i den forstand at den gjør det mulig å lage scenarioer som illustrerer utfordringene knyttet til hybride trusler og dermed bidra til å besvare problemstillingen for oppgaven. Elementene i analysen er hver for seg basert på reelle hendelser, og har dermed en rot i virkeligheten. Resultatene vurderes som realistiske, om enn ganske dramatiske. Dramatikken er en følge av definisjonen for samfunnssikkerhet som ble lagt til grunn i kapittel 3: *ekstraordinære* påkjenninger og tap, høy *kompleksitet* og *gjensidig avhengighet* samt potensiale for å *undergrave tillit til vitale samfunnsfunksjoner*. Rammene for oppgaven tillater derimot ikke å vurdere i hvilken grad de er sannsynlige. Tankeprosessen rundt utvalget av metoder, virkemidler og verktøy er forsøkt beskrevet og begrunnet, så resultatet bør være både forståelig og velbegrunnet. Dette betyr imidlertid på ingen måte at dette er den *eneste* måten komponentene i en hybrid trussel kan modelleres. Resultatet kan neppe kalles dekkende eller uttømmende. Dette kravet er vanskelig å oppfylle, siden det finnes et nærmest uendelig antall og kombinasjoner av virkemidler og verktøy som kan brukes for å legge press på en annen

stat. Det samme gjelder kravet om at resultatet skal være gjensidig utelukkende. Det er fullt mulig å diskutere plasseringen av enheter som er gjort. Det er for eksempel enkelt å argumentere for at "implisert økonomisk tvang" primært er en politisk metode eller at det handler om informasjonsoperasjoner. Den endelige vurderingen er at det er viktigere at resultatet er praktisk brukbart enn at det er uttømmende og gjensidig utelukkende.

Metode	Virkemiddel	Verktøy
militært	offensiv militær operasjon	konvensjonelle styrker, spesialstyrker
	militært press	kjernefysiske styrker, konvensjonelle styrker, spesialstyrker
politisk	multilateralt diplomati	diplomati
	bilateralt (tvangs)diplomati	diplomati
	støtte stedfortredergrupper	diplomati, NGO, næringsliv, etterretningstjeneste
	public diplomacy	stedfortredergrupper, etterretningstjeneste, diplomati, redigerte medier, sosiale medier
	manipulere internasjonal rett	diplomati, rettsvesen
	utforming av lover	rettsvesen
	rettsforfølge nasjonalt	rettsvesen
informasjon	propagandaoperasjon	stedfortredergrupper, etterretningstjeneste, diplomati, redigerte medier, sosiale medier
	desinformasjon	stedfortredergrupper, etterretningstjeneste, diplomati, redigerte medier, sosiale medier, hackergrupper
økonomisk	sanksjoner	diplomati
	valutaspekulasjon	næringsliv
	implisert økonomisk tvang	organisert kriminalitet, diplomati, næringsliv
fordekt	fordekte operasjoner	spesialstyrker, organisert kriminalitet, stedfortredergrupper, etterretningstjeneste
	vold v/stedfortreder	organisert kriminalitet, stedfortredergrupper, etterretningstjeneste
	cyberangrep	konvensjonelle styrker, organisert kriminalitet, etterretningstjeneste, hackergrupper

4.2 Scenarioer

Med bakgrunn i den morfologiske analysen presenteres tre scenarioer som på forskjellige måter beskriver tenkte hybride trusler som Norge kan utsettes for. Scenarioene er tenkbare, men ikke nødvendigvis sannsynlige. Det er lagt vekt på å gjøre scenarioene komplekse og realistiske. For å unngå uintendert stigmatisering brukes fiktive navn på statene som har rollen som trusselaktør. Hendelsestypene etterretningsvirksomhet og informasjonsoperasjoner er stadig pågående aktiviteter som finnes i alle tre scenarioer.

4.2.1 Scenario 1: "Kamp om sannheten og ressursene"

En sabotasjeaksjon mot norsk gasseksport til utlandet gjennomføres av en hackergruppe med bånd til en fremmed stat. Gassanlegget som rammes er del av et EU-finansiert prosjekt som etablerer nye rørledninger fra Norge for å gjøre europeiske land mer uavhengige av gasseksport fra den fremmede staten. Parallelt med rørledningen er det også bygget opp terminaler for mottak av LNG-gass fra USA som transporteres på kjøl. Den fremmede staten har flere ganger protestert mot den urettferdige konkurransen som de utsettes for, som har ført til økende arbeidsledighet og misnøye internt i landet.

Aksjonen utføres via en "innsider" hos en underleverandør med aksess til styringssystemene som presses til å laste inn skadevare. Blant annet har denne personens sensitive helseopplysninger kommet på avveie, og blitt brukt som pressmiddel for å få vedkommende til å samarbeide. Skadevaren ødelegger ikke bare det logiske nettverket, men også fysisk infrastruktur i ledningssystemet. En ukontrollert gassutblåsning fra gassanlegget fører til panikk i lokalsamfunnet og evakuering av lokalbefolkningen. Parallelt med utblåsningen mottar personer som bor i nærheten av to tilsvarende anlegg i Norge falske SMS-beskjeder som advarer om at tilsvarende utblåsninger er ventet også fra disse anleggene. Beskjedene er utformet som om de kommer fra DSB.

Et oljeselskap fra den fremmede staten plasserer et boreskip innenfor fiskevernsonen ved Svalbard. Skipet er ledsaget av kystvaktfartøyer fra den fremmede staten. Kystvaktfartøyene påstås å være i området for å drive fiskerioppsyn, men observasjoner tyder på at det også er militært personell om bord. Norge protesterer. EU-landene er lite villige til å støtte de norske protestene, blant annet på grunn av uløste konflikter om fiskerettigheter.

Den administrerende direktøren for et norsk firma som opererer i den fremmede staten arresteres, anklaget for korrupsjon og spionasje. Flere andre i firmaets ledelse settes på Interpols liste over ettersøkte. Virksomhetssensitiv informasjon hentes ut av firmaets nettverk, og deler av dette blir publisert på Wikileaks for å sverte ledelsen og norske myndigheter. Firmaets hovedkvarter i Norge har tidligere vært utsatt for cyberangrep, der sensitiv informasjon om deres teknologi har blitt stjålet.

4.2.2 Scenario 2: "Sivile inngrep, aktiv infiltrasjon"

I en fremmed stats medier blir det over tid fokusert på Norge som et land der fascismen blomstrer. En fjernsynsserie fokuserer på ulike historiske eksempler som fornorskningen av samene, Nasjonal samling, jødetransportene, 22/7-angrepene, bruk av Barnevernet for å ”stjele” utenlandske barn i den hensikt å styrke genene til det norske folk, siden de er truet av innvandring fra Asia og Afrika. Budskapet er at «fascismen» har dype røtter i Norge, og aldri egentlig har blitt bekjempet. Det eneste terrorangrepet som har skjedd i Norge var utført av en

etnisk norsk «fascist». Det er flere aktuelle og betente saker mellom Norge og den fremmede staten, blant annet oppkjøp av et større landområde fra en privat norsk aktør og etablering av et bilateralt forskningssenter som norske myndigheter mistenker for direkte knytninger til den fremmede statens forsvarsdepartement. Den utenlandske aktøren i prosjektet har fått skattefordeler og billige lån fra den fremmede staten for etableringen i Norge.

I småbyen Bakkefjord, ikke langt fra grensen, arrangerer en norsk gruppe med bånd til den fremmede staten en demonstrasjon. Den består av personer fra den fremmede staten tilhørende en høyreradikal gruppe, men deltagerne inkluderer også personer fra samme land med bosted i Norge. En del av disse er barnefamilier. En kjent radikal nasjonalistisk politiker fra den fremmede staten dukker uventet opp i Bakkefjord og holder en appell der han oppfordrer han til motstand mot norsk diskriminering av sine landsmenn og motarbeiding av ønsker om å utvikle tettere næringssamarbeid. En større politistyrke blir sendt til stedet for å holde kontroll på demonstrasjonen. Det oppstår håndgemeng, noe som blir bredt rapportert i utenlandske medier som et eksempel på norske myndigheters fiendtlige innstilling. En del av demonstrantene tar seg inn på den lokale politistasjonen, der en norsk polititjenestemann blir skutt og drept og flere blir skadet. Beredskapstroppen sendes med fly fra Oslo, men når de lander i Bakkefjord møtes de av væpnet sivilt personell på den lokale flyplassen. Det kommer til skuddveksling, og etter hvert klarer beredskapstroppen å få kontroll over flyplassen.

I løpet av de to foregående dagene har drikkevannet i Åmot kommune blitt forgiftet med en hittil ukjent og kraftig tarmbakterie. Dette har rammet både lokalbefolkningen og en stor del av styrkene til Forsvarets Spesialkommando i Rena leir. Andre deler av spesialstyrkene deltar i internasjonale operasjoner, og er ikke tilgjengelige på kort varsel.

Dagen etter blir en gruppe turister fra den fremmede staten angrepet av maskerte menn med skytevåpen under en omvisning i Frognerparken. 10 turister blir drept. En ukjent og tilsynelatende høyreradikal terrorgruppe tar på seg ansvaret for angrepet. PST og E-tjenesten avdekker at gruppen i realiteten består av spesialsoldater fra den fremmede staten.

4.2.3 Scenario 3: "Militære trusler"

Norske myndigheter har etter en økonomisk krise som har medført store kutt i forsvarsbudsjettet tillatt allierte maritime overvåkingsfly å operere ut fra norske baser, noe som har ført til protester fra en fremmed stat. Marinefartøyer fra de Norges allierte operer også langt oftere enn tidligere i deres nærområder. Det er sterk innenrikspolitisk retorikk i landet, der nasjonalistiske krefter krever at presidenten tar affære for å sikre nordvestflanken. En langvarig propagandakampanje som peker på at norsk sikkerhetspolitikk har bidratt til å forrykke maktbalansen i nord. Norske protestgrupper oppstår, finansiert av nabolandet.

Den fremmede staten gjennomfører gjentatte store ikke-varslede militærøvelser, inkludert aktivering av A2AD-systemer i perioder. Dette medfører blant annet at flytrafikk internt i Norge må innstilles. Det kommer også uttalelser fra ambassaden i Oslo om at Norge kan bli mål for atomvåpen. Det lekkes informasjon til norske medier om at ambassaden har testet sine planer for evakuering av personell i tilfelle en krise skulle oppstå.

5. Drøfting

Som scenarioene viser, vil en hybrid trussel kunne rettes inn mot ulike samfunnssektorer – militær så vel som sivil, privat så vel som offentlig. Varslingstiden kan være kort, og hovedhensikten med en hybrid trussel vil være å skjule selve hovedaktøren, dennes bakenforliggende hensikt og å forsinke forsvarerens beslutningsprosesser. De konkrete målene kan finnes på ulike steder i samfunnet, avhengig av hvilke sårbarheter det aktuelle landet har. Utviklingen blant annet innen IKT og media samt globaliseringen av verdensøkonomien gir trusselaktører et bredere utvalgt av instrumenter og flere innfallsvinkler til å bruke disse instrumentene mot målenes sårbarheter. Den første delen av drøftingen omhandler deteksjon av en del av enkelthendelsene i scenarioene. Denne gjennomgangen er primært knyttet til det operative nivået i den norske modellen for krisehåndtering. I den avsluttende delen av drøftingen rettes oppmerksomheten mot utfordringer på strategisk nivå, der det totale bildet samles for beslutningstagerne.

5.1 Deteksjon av separate hendelser i scenarioene

Hendelsestypene i scenario 1 omfatter først og fremst etterretningsvirksomhet som danner grunnlag for sabotasjeaksjoner (cyberangrep og verving av en innsider i en norsk virksomhet av strategisk betydning knyttet til gasseksport). En gassutblåsning med konsekvenser for lokalsamfunnet blir en følgehendelse av cyberangrepet. Det første cyberangrepet rammer en norsk virksomhet i Norge. I den andre hendelsen rammes en norsk virksomhet i utlandet av et datainnbrudd der informasjon hentes ut og publiseres for å ramme virksomhetens omdømme.
Scenario 1 fokuserer også på at Norges relasjoner til partnere og allierte blir utfordret gjennom informasjonsoperasjoner og cyberangrep. Scenario 2 bringer in problematikk som stedfortredergrupper, strategiske oppkjøp, sabotasje mot drikkevann og terrorangrep som en *false flag*-operasjon. Scenario 3 bringer inn den militære dimensjonen i form av militært press mot Norge.

Deployering av boreskipet og aktiviteten til kystvaktfartøyene fra den fremmede staten i scenario1 kan bli detektert av Forsvaret generelt og E-tjenesten spesielt, men håndteringen vil trolig skje i regi av UD. De vil imidlertid også ha en sikkerhetspolitisk dimensjon (ref. Elektron-saken i 2005 beskrevet av Fermann 2010:36). Urettmessig rettsforfølging av nordmenn i utlandet vil også være en sak som primært håndteres av UD. I scenario 2 er oppkjøp av landområder en problematikk. Norges økonomi er svært åpen, spesielt i forhold til petroleumseksport og forvaltning av Statens pensjonsfond utland. Økonomi er derfor en viktig faktor for norsk nasjonal sikkerhet (Fermann 2010:28). Finansministeren har trolig derfor en fast plass i RSU (JBD 2016:182). Disse hendelsestypene vil av plasshensyn ikke bli drøftet mer inngående i denne oppgaven.

5.1.1 Etterretningsvirksomhet

Selv om fremmed etterretning vil finne mye åpent tilgjengelig informasjon, spesielt i liberale vestlige demokratier, har kontraetterretning et viktig oppdrag i å detektere og motvirke trusselaktørens rekrutteringsvirksomhet og hans innhenting av informasjon om forsvarerens sårbarheter. I en krisesituasjon vil effektiv kontraetterretning hindre trusselaktøren i å hente inn oppdatert informasjon om effekten av tiltakene som er satt i verk for sin egen «battle damage assessment» (Cederberg og Eronen 2015:7). I scenario 1 har det pågått etterretningsvirksomhet over lang tid for å kartlegge systemsårbarheter hos virksomheten som eier gassanlegget, samt

sårbarheter hos personell som har aksess til kritiske systemer. Verdiskapningen fra eksport av olje og gass er av stor betydning for Norge, og bortfall av disse inntektene vil få negative følger for den norske velferdsmodellen, og dermed kunne ramme både sosial samhørighet og politisk stabilitet (Fermann 2010:55). Norsk infrastruktur for telekommunikasjon har også vært kartlagt over tid. Det er utfordrende å knytte skadevirkningene av etterretningsvirksomhet til konkrete konsekvenser som for eksempel økonomisk tap. Langvarig innsamling vil på sikt føre til at en motstander får et godt bilde av det han har behov for å vite. Sikkerhetspolitisk vil konsekvensene av etterretningsvirksomhet først åpenbare seg i en reell krise, for eksempel gjennom en sabotasjeaksjon (JBD 2016:92). Deteksjon av fremmed etterretningsvirksomhet er en av PSTs hovedoppgaver (PST u.å.). I dag erkjenner politiske myndigheter at PST mangler evne til å forebygge og etterforske digital spionasje og sabotasjeforsøk på en tilfredsstillende måte, og har bevilget midler for styrking på dette området (JBD 2016:180). NSM fokuserer på å forebygge og begrense skade, mens PST og E-tjenesten bruker NSMs funn i der videre arbeidet med å finne ut hvor trusselen kommer fra (Kvamme 2017). De tre tjenestene har i flere år advart om at etterretningsvirksomhet er en alvorlig trussel, og at virksomheten mot Norge blir stadig mer aggressiv og målrettet (E-tjenesten 2017:34). Etterretningsvirksomheten er særlig rettet mot forsvars- og beredskapssektorene, politiske beslutningsprosesser og kritisk infrastruktur (PST 2017:7). Tradisjonelle metoder som HUMINT er fremdeles aktuelle, men PST har gjennom flere år advart om at flere stater utvikler evne til digital spionasje (PST 2017:9). NSM konstaterer også at antallet cyberangrep fra avanserte aktører øker i omfang (NSM 2017:17). Såkalt statlig industrispionasje er en faktor i forhold til teknologisektoren. Det er i enkelte land tette bånd mellom etterretningstjenester og næringsliv, og dermed kan statlige etterretningsressurser benyttes for å støtte eget næringsliv. I trusselvurderingen for 2011 pekte PST på utfordringene som er knyttet til økende internasjonalisering av norsk næringsliv og forskning, samt tjenesteutsetting av oppgaver til andre land. Dette medfører at flere får tilgang til skjermingsverdig informasjon. Eksempelet i scenario 1 viser hvordan personopplysninger i en gitt situasjon kan benyttes for å ramme nasjonale sikkerhetsinteresser, og illustrerer sårbarheten som lange og uoversiktlige verdikjeder på IKT-området representerer (JBD 2015a:15). Helseopplysninger er sensitive, men ikke sikkerhetsgraderte. Tjenesteutsetting på IKT-området og skylagring fører til økt sårbarhet, og siden informasjonen er mangfoldig vil skjerming kreve en fleksibel or risikobasert tilnærming (*ibid.*:84). NITO påpeker at det fremdeles vil være opp til

enkelte departementer, for eksempel OED og HoD å definere når deres område omfattes av sikkerhetsloven. Dermed vil behandling av sensitiv informasjon i ugraderte nettverk, for eksempel helsedata, havne i en gråsone (NITO 2017).

5.1.2 Trusler i det digitale rom

Trusler i det digitale rom omfatter både fremmed etterretningsvirksomhet og potensiell sabotasje. E-tjenesten benytter ikke begrepet hybride trusler, men beskriver hvordan digital sabotasje inngår i et overordnet konsept sammen med desinformasjon, manipulasjon, propaganda og stimulering av sosial uro for å diskreditere andres styresmakter, forvirre befolkningen og demoralisere militært personell (E-tjenesten 2017:34). Vedvarende kartlegging av sårbarheter, for eksempel kritisk kommunikasjonsinfrastruktur og kritisk personell som jobber med dette er viktige aktiviteter som understøtter eventuelle fremtidige sabotasjeaksjoner (E-tjenesten 2017:35, Nkom 2016:25). Det er betydelige mangler i den nasjonale evnen til å detektere digitale trusler. I forrige avsnitt er det pekt på at PST skal styrke sin evne til å forebygge og etterforske trusler i det digitale rom. NSM/NorCERT opererer som tidligere omtalt Varslingsnettverk for Digital Infrastruktur (VDI). VDI er et sensornettverk som skal detektere forsøk på innbrudd mot kritisk infrastruktur, og er basert på samtykke fra de virksomhetene der sensorene er utplassert (Lysne II 2016:23). Dette betyr at trusler som rettes mot aktører uten en VDI-sensor ikke vil bli detektert på denne måten. NSM (2017:17) peker på en ny trend der avanserte trusselaktører angriper mindre norske virksomheter med sårbare IKT-systemer for å etablere et "brohode" som utgangspunkt for å angripe det egentlige målet. De mest avanserte truslene blir også stadig mer kompliserte å detektere på grunn av kryptering og på grunn av at IP-adresser blir mindre og mindre relevante (Lysne II 2016:23). Lysne II-utvalget har slått fast at E-tjenestens fremtidige evne til å levere etterretninger og dermed beslutningsstøtte om alvorlige trusler mot rikets sikkerhet avhenger av aksess til de kommunikasjonskanalene der slike trusler planlegges og gjennomføres (Lysne II 2016:11). Utvalget anbefaler at tjenesten gis tilgang til datastrømmer som krysser landegrensene, hovedsakelig i fiberoptiske kabler. Denne nye kapabiliteten omtales som Digitalt grenseforsvar (DGF). I kapittel 3 ble det pekt på at reformer på etterretningsområdet ofte anbefaler investering i bedret innsamling. Analysekapasiteten og koordineringen av arbeidet med digitale trusler er også forbedret gjennom opprettelsen av Cyber koordineringssenter (FCKS). Tjenestene som deltar (NSM, PST, E-tjenesten, Kripos) vil imidlertid fortsatt jobbe på

sine egne mandater, og det er ikke kjent hvordan utfordringer knyttet til informasjonsdeling vil bli håndtert i senteret.

Cyberangrepet mot et gassanlegg i scenario 1 *kan* bli detektert gjennom VDI dersom anlegget deltar i dette samarbeidet. Hendelsen illustrerer viktigheten av tett samarbeid mellom statlige etater og private virksomheter. E-tjenesten har i dag marginal evne til å gi forvarsel om slike angrep, men kan gjennom sitt internasjonale samarbeid bidra med informasjon som kan peke NSM i riktig retning. Slik informasjon er i følge Lysne II (2016:23) den viktigste faktoren for NSMs deteksjon av avansert trusler. Imidlertid er slik informasjon kun et biprodukt av samarbeidende tjenesters virksomhet, de kommer ofte sent, og norske myndigheter er dermed sårbare både politisk og i et suverenitetsperspektiv (*ibid.*:29). I scenario 1 beskrives også et datainnbrudd mot en norsk virksomhet i utlandet. UDs evaluering av norske myndigheters krisehåndtering i forbindelse med In Amenas-angrepet slår fast at det er vertslandet som har ansvar for sikkerheten til de som oppholder seg på landets territorium. Norske myndigheter strekker seg langt for å bistå nordmenn i utlandet, men er avskåret fra myndighetsutøvelse på et annet lands territorium (UD 2013:6). Næringslivets sikkerhetsråd (NSR) understreker sikkerhetsutfordringer knyttet til internasjonalisering av norsk næringsliv, og behovet for at bedrifter som opererer i risikosoner har gode beredskapsrutiner som er fundert i risikovurderinger (Beitland 2013). Granskingsrapporten etter In Amenas-angrepet viser at generell informasjon om den generelle sikkerhetssituasjonen i Algerie fantes, men at taktisk varsling om hvor og når en angriper kan slå til ikke er noe private aktører kan forventes å frembringe for sin virksomhet (Statoil ASA 2013:55), samt at dialog med statlige myndigheter derfor er nødvendig for å bedre samarbeidet rundt aksess til og bruk av informasjon knyttet til trusler og security (*ibid.*:78). Lindén (2015:107) viser at norske myndigheters sikkerhetsrådgivning til virksomheter varierer i regularitet, omfang og detaljgrad, samt at NSR spiller en viktig rolle som kontaktpunkt mellom myndigheter og virksomheter. Regjeringen peker også på behovet for å etablere bedre informasjonsutveksling om trusler, sårbarheter og risiko mellom statlige etater og næringslivet.

5.1.3 Informasjonsoperasjoner

NSM (2017:37) påpeker at Norge til forskjell fra andre land, mangler en funksjon for deteksjon av desinformasjon og forsøk på påvirknings og informasjonsoperasjoner. Påvirkningsoperasjoner omtales av NSM i Risiko 2017 for første gang, noe som reflekterer den økte oppmerksomheten mot denne utfordringen opp mot Stortingsvalget i 2017. I et foredrag i februar 2017 om Totalforsvaret påpekte DSB-direktør Cecilie Daae at informasjonsoperasjoner er et område DSB tenker å ta et særlig ansvar for, siden de også har ansvar for risiko- og krisekommunikasjon, inkludert ut mot befolkningen. Viktige oppgaver vil være å øke bevisstheten rundt trusselen i befolkningen, utvikling av scenarioer og en nasjonal strategi for håndtering av truslene (DSB 2017). Dette er imidlertid tiltak som i stor grad handler om å håndtere konsekvenser, og mindre om å direkte legge til rette for bedre deteksjon, og er således i tråd med DSBs mandat om å se på de store linjene. Eksempelet i scenario1 med falske SMS-beskjeder viser at sårbarheter i ekom-infrastrukturen også vil være en aktuell angrepsvektor for en trusselaktør som ønsker å påvirke befolkningen og undergrave myndighetene[24]. DSB-direktøren viste i foredraget til Sverige, der Myndigheten för samhällsskydd och beredskap (MSB) siden 1950-tallet har arbeidet med psykologisk forsvar (MSB u.å.). NSM (2017:36) peker også på lignende tiltak i Tsjekkia, Innenriksministeriets *Centre Against Terrorism and Hybrid Threats* (MVČR 2017) og i Finland under ledelse av regjeringens kommunikasjonsavdeling, som har ansvar for strategisk kommunikasjon (Statsrådets kansli u.å.). I EU har East StratCom Task Force i oppgave å motvirke russiske desinformasjonskampanjer gjennom blant annet å bygge opp EUs evne til å forutsi og håndtere og respondere på desinformasjon fra eksterne aktører (EEAS 2017). Det finnes i tillegg en rekke ikke-statlige aktører og tenketanker som for eksempel Bellingcat.com og Securingdemocracy.org som følger og analyserer desinformasjonskampanjer. Den ideelle organisasjonen Faktisk.no jobber med faktasjekk av samfunnsdebatten i Norge, og har ikke fokus på det internasjonale bildet. Forsvarets siste langtidsplan (FD 2016a:36) påpeker behovet for samordning og koordinering av tiltak som forsvarssektoren utøver i informasjonsdomenet. Dette omfatter forsvarssektorens evne til å identifisere og analysere informasjonsoperasjoner rettet mot

[24] EkomROS 2017 inneholder også et lignende scenario der norske internettbrukere ledes til falske nettsider med manipulerte nyheter ved hjelp av målrettet og avgrenset DNS-spoofing som er vanskelig å detektere raskt, men er av tilstrekkelig omgang til at informasjon kan spres videre i sosiale medier og bidra til undergraving av norske myndigheter (Nkom 2017:25).

Norge på et tidlig stadium, samt til å understøtte politiske og militære målsetninger med egen strategisk kommunikasjon. Langtidsplanen konstaterer videre at strategisk kommunikasjon krysser etablerte skillelinjer både internt i forsvarssektoren og tverrsektorielt, og at effektiv organisering på området vil være utfordrende både organisasjonsmessig og prinsipielt. I Stortingsmeldingen om samfunnssikkerhet (JBD 2016:92) knyttes informasjonsoperasjoner og forsøk på påvirkning av politiske prosesser mot fremmed etterretningsvirksomhet i Norge. Meldingen inneholder imidlertid ikke konkrete forslag for å styrke arbeidet med deteksjon av informasjonsoperasjoner spesifikt, men fokuserer på tiltak som å bevisstgjøre allmenheten og virksomheter ved hjelp av mer samordnede ugraderte trusselvurderinger, effektivisering av arbeidet med personellsikkerhet for å motvirke innsidetrusselen, bedre E-tjenestens aksess til digital kommunikasjon, bedre samordning gjennom FCKS og mer effektiv utveksling av trussel- og risikoinformasjon mellom statlige etater og næringslivet (*ibid.*:93). Denne tilnærmingen illustrerer hvordan komplekse risikoer håndteres ved bred involvering av aktører både på tvers av statlige sektorer, mellom statlige og private aktører og ved involvering av befolkningen som beskrevet i *Stakeholder Involvement Model* i kapittel 3. Internasjonalt samarbeid vil også bedre evnen til deteksjon av informasjonsoperasjoner. Dette kan skje både ved å benytte informasjon fra frivillige aktører som beskrevet, men også gjennom samarbeid i NATO og EU-sammenheng. Regjeringen har som et eksempel besluttet at Norge skal slutte seg til det finsk-ledete *European Centre of Excellence for Countering Hybrid Threats* i Helsinki (SMK 2017b

5.1.4 Stedfortredergrupper og voldelige aksjoner

Stedfortredergrupper som opererer i Norge er en mangfoldig kategori. I scenario 2 omtales en norsk gruppe med bånd til og sympatier for en fremmed stat. Demonstrasjonen som gruppen arrangerer består av lokale personer med opprinnelse fra en fremmed stat, men forsterkes også av representanter for en utenlandsk radikal og voldelig gruppe. Slik hendelsene er beskrevet, vil de falle inn under virksomheten til PST og Politiet. Deteksjon av grupper i Norge som kan ha et voldspotensiale og som har bånd til en fremmed stat vil trolig primært være koblet til PSTs mandat om kontraetterretning og kontraterror. PST vurderer det som lite sannsynlig at høyreekstreme grupper vil utføre en terrorhandling i Norge i 2017, men konstaterer at bedre organisering og koordinering i disse miljøene, inkludert kontakter med utlandet er en økt bekymring (PST 2017:17). Både PST og E-tjenesten har kontraterror som en viktig oppgave og

samarbeider i FKTS. Det andre relevante samarbeidsorganet er FCKS som ledes av NSM, og der også Kripos er representert. FCKS presenteres som ett av tiltakene for håndtering av fremmed etterretningsvirksomhet mot norske interesser (JBD 2016:94), noe som illustrerer den tette koblingen mellom etterretning og trusler i det digitale rom. Grupper som støtter fremmede stater kan detekteres av PST. I scenario 2 viser det seg at tilsynelatende sivile som angriper en politistasjon kan være utenlandske militære styrker uten kjennemerker. I dette tilfellet er spørsmålet om og når ansvaret overføres til Forsvaret. Stedfortredergrupper som arrangerer demonstrasjoner kan bli detektert som et lov- og orden-problem og håndtert av Politiet. Etterretning, PST, Kripos, internasjonalt politisamarbeid, politiets egen etterretningsvirksomhet kan gi et forvarsel og kanskje få informasjon om at grupper har tilknytninger til fremmede stater. PST spiller en viktig rolle her.

5.1.5 Konvensjonell militær operasjon

Hendelsene i scenario 3 er ikke et militært angrep, men militært press for å påvirke norske sikkerhetspolitiske prioriteringer. Johansen (2006:38) påpeker at både politisk og teknologisk utvikling kan gjøre militær maktbruk mot Norge fra Russland og andre stater om ikke sannsynlig, så i hvert fall mulig. Deteksjon av og varsling om ytre trusler er en av E-tjenestens hovedoppgaver. I Fokus 2017 konstaterer tjenesten at Russland har fått både økt vilje og evne til å hevde sine utenrikspolitiske interesser. Dette inkluderer høyteknologiske kapasiteter som utfordrer vestlige forsvarssystemer og begrenser norsk og alliert handlefrihet i våre nærområder. Sivil og militær norsk kritisk infrastruktur befinner seg nå innen rekkevidde av russiske missilsystemer med høy presisjon (E-tjenesten 2017:13, 14, 28).

5.1.6 Sabotasje mot drikkevann

Sabotasje mot drikkevann vil trolig ikke nødvendigvis umiddelbart klassifiseres som en tilsiktet hendelse. Norge har flere tusen vannverk av ulike størrelse, og det er vannverkseier som er ansvarlig for å avgjøre om en hendelse er et driftsavvik eller en alvorlig beredskapssituasjon (Mattilsynet 2017:2). Ved mistanke om at det foreligger en helsefare, skal vannverkseier varsle Mattilsynet og kommunelege/smittevernlege, samt ha dialog med Brannvesenet om varsling. Brannvesenet vil i en ulykkessituasjon stanse eller begrense akutt forurensning, eventuelt med assistanse fra Interkommunalt utvalg mot akutt forurensning (IUA) og Kystverket. Det er også etablert varslingsrutiner mellom Mattilsynet og Folkehelseinstituttet. Politiet har gjennom

Politiloven en viktig rolle i å opprettholde offentlig orden og sikkerhet, samt yte hjelp til borgerne i faresituasjoner (*ibid.*:22-23). På et tidspunkt kan man anta at Nasjonalt sivilt situasjonssenter vil bli varslet om hendelsen gjennom rapportering fra for eksempel DSB eller POD. Forsvaret gjennom SITSEN vil trolig også bli gjort klar over at hendelsen har konsekvenser for militære avdelinger. Departementsråden i HoD har fast plass i Kriserådet.

5.2 Deteksjon av koordinering

Hendelsene beskrevet ovenfor er alvorlige nok, men vil ikke hver for seg kunne kalles en hybrid trussel. Trusselen blir hybrid når koordinert bruk av ulike virkemidler mot identifiserte sårbarheter kobles med en politisk ambisjon om å destabilisere et annet land uten at det bryter ut en åpen konflikt. Overraskelsesmomentet, villedning og politisk fornektbarhet vil prege situasjonen. Iverksettelse av et hybrid angrep krever grundig planlegging basert på lengre tids kartlegging motstanderens sårbarheter. Trusselaktørens etterretningsapparat spiller her en sentral rolle. Dernest er effektiv koordinering mellom ulike beslutningsnivåer og på tvers av ulike sektorer en forutsetning. Det må finnes en politisk vilje og evne til å forplikte ressurser i tilstrekkelig omfang fra ulike sektorer. En sentralstyrt (og autoritær) stat vil her ha et fortrinn med tanke på effektiv koordinering og tildeling av ressurser. Informasjonsoperasjoner rettet mot hjemmepublikummet, befolkningen i mållandet og internasjonal opinion vil foregå både i forberedelses- og gjennomføringsfasen.

Avsnitt 3.1 omhandlet etterretningsfunksjonens bidrag i deteksjon og varsling av trusler gjennom *monitorering* av kjente parametere og *discovery* av ukjente farer som kan inntreffe i fremtiden. Beskrivelsen av hybride trusler i avsnitt 3.2 og scenarioene inneholder mange elementer som kan monitoreres, som fremmed etterretningsaktivitet i ulike domener, digitale trusler, fremmed militær aktivitet og ulike former for stedfortredergrupper, enten de representerer en voldstrussel eller er involvert i undergravende virksomhet. De norske sikkerhetsinstitusjonene har som diskutert varierende evne til monitorering, men dette er "kjente fenomener" som blant annet presenteres i ugraderte årlige trussel- og risikovurderinger. En av utfordringene hybride trusler er imidlertid at velkjente trusler manifesterer seg i nye og uventede settinger, noe som gjør en risikotilnærming viktig ved siden av trusseltilnærmingen. Trussel- og risikovurderingene er samtidig et uttrykk for norske myndigheters trusselpersepsjon. Det er videre pekt på trekk ved

hybride trusler som gjør deteksjon og beslutningstagning komplisert: tvetydigheten som skapes ved at skillet mellom krig og fred blir utydelig, organisatoriske utfordringer som evne til tverrsektoriell koordinering i møte med en trussel som rettes mot nettopp denne sårbarheten, hybride truslers "krypende" karakter og det at trusselen er befolkningssentrisk på den måten at den søker å påvirke faktorer som befolkningens motstandsvilje og forholdet mellom etniske eller sosiale befolkningsgrupper.

5.2.1 Trusselaktørens intensjoner

Trusselaktørens intensjoner, den politiske ambisjonen om å destabilisere, representerer en særlig utfordring. Hybride trusler er en tilnærming som (vestlig) litteratur gjerne knytter til autoritære stater, der kretsen av de som deltar i beslutningsprosessen gjerne er svært begrenset. Dette leder inn i *discovery*-domenet. Hvordan kan man fastslå intensjonen til lederen i et annet land? Ben Israel (1989:691) påpeker to problemer. For det første vanskelighetene knyttet til å lese persons tanker, eller sagt på en annen måte, aksess gjennom relevante etterretningskapasiteter. For det andre, man behøver ikke bare å kjenne motpartens intensjon her og nå, men også i fremtiden. Selv om man klarer å avdekke at lederen i et annet land planlegger å angripe i løpet av 24 timer, hvordan kan vi vite at han ikke vil ombestemme seg i løpet av denne tiden? Et svar på dette dilemmaet ligger i monitorere kjente indikatorer. Grabo (2015:25) peker på tre hovedkilder for kunnskap når en indikatorliste skal bygges: i) logikk eller historisk presedens, ii) spesifikk kunnskap om en stat eller gruppe av staters militærdoktrine og praksis, iii) lærdom fra en stat eller grupper av staters oppførsel i en nylig krig eller internasjonal krise. Logikk eller historisk presedens peker på at en stat alltid vil måtte gjøre visse forberedelser før den kan gå til væpnet konflikt – offensive og defensive militære tiltak, forberedelse av befolkningen og verdensopinionen, økonomiske tiltak. Militære og politiske doktriner og praksis gir mer spesifikk kunnskap om det aktuelle landets trolige handlinger. Lærdom fra en reell krisesituasjon vil være verdifullt for å underbygge det teoretiske grunnlaget, selv om slik kunnskap ikke alltid vil være tilgjengelig, og selv om ingen krisesituasjoner vil være like (*ibid.*:26- 27).

5.2.2 Tvetydig trussel

Både *Failure of foresight*- og HRO-teoriene legger vekt på informasjonsdeling og –forvaltning i sikkerhet- og beredskapsarbeid. Rutinemessig koordinering og kommunikasjon horisontalt

mellom enheter på samme nivå og i vertikalt i kommandokjeden danner grunnlaget for god situasjonsforståelse også i en krise. Strukturelle endringer i justissektoren har for eksempel ført til bedre kommunikasjon og koordinering etter 22/7 (Albrechtsen et. al. 2017:17). Nye arenaer for samhandling mellom etterretnings- og sikkerhetstjenestene er etablert gjennom FCKS og FKTS (der tjenestene fortsatt skal jobbe på egne lovgrunnlag, noe som medfører at eventuelle legale skranker for samarbeid og informasjonsutveksling består), og ledelsen for de samme tjenestene har plass i RSU, og kan inkluderes i Kriserådet ved behov.

Rinelli og Duyvesteyn (2017:34) peker på at tenkningen rundt håndtering av hybride trusler i stor grad handler om sivil-militært samvirke. Det norske totalforsvarskonseptet har gjennomgått en modernisering fra å gjennom den Kalde krigen primært å handle om det sivile samfunnets støtte til Forsvaret under den Kalde krigen, til å i dag å omfatte gjensidig støtte og samarbeid mellom de to sektorene i hele krisespekteret, fra fred via sikkerhetspolitiske kriser til væpnet konflikt. Utviklingen henger sammen med en endret sikkerhetspolitisk situasjon og økt vekt på samfunnssikkerhet (Kristoffersen 2006). Støtte innenfor rammen av Totalforsvaret er ikke lenger avhengig at beredskapslovgivningen[25] trer i kraft (FD 2015a:12). Det kan synes som om det finnes gråsoner mellom ansvarsområdene til sivil og militær sektor. Forsvarets rolle er ikke tydelig definert i JBD-publikasjonene som er brukt i denne oppgaven. Knutsen (2010:373) peker på at løst definerte grenselinjer i de sivil-militære relasjonene kan skape uklarhet i en krisesituasjon. Men på den andre siden kan gråsoner bety manøvreringsrom og fleksibilitet, noe som kan være en fordel for håndtering av hybride trusler. Fleksibilitet er et viktig trekk ved HRO-organisasjoner, og et viktig virkemiddel for å håndtere hybride trusler preget av tvetydighet (IISS 2016:2, Jagello 2000 2016:18). Proposisjonen om ny sikkerhetslov legger opp til en fleksibel lov for å møte et dynamisk sikkerhetsbilde (FD 2017a:7), og behandlingen av sikkerhetsspørsmål på strategisk nivå i RSU og Kriserådet legger også opp til fleksibilitet i form av hvilke etater som deltar (JBD 2016:182). Scenarioene er som nevnt ikke uttømmende, og det

[25] De mest sentrale beredskapslovene er: Beredskapsloven av 15. desember 1950; Næringsberedskapsloven av 16. desember 2011; Rekvisisjonsloven av 29. juni 1951; Vernepliktsloven av 17. juli 1953; Lov om beredskapslagring av petroleumsprodukt av 18. august 2006; Drivstoffanleggloven av 31. mars 1949; Skipsrekvisisjonsloven av 19. desember 1952; Helseberedskapsloven av 1.juli 2001; Sivilbeskyttelsesloven av 25. juni 2010 (Forsvardepartementet 2015:30).

er vanskelig å tenke seg at en stat skal kunne ha planverk som dekker alle mulige eventualiteter av tilsiktede og utilsiktede hendelser som kan ramme. Man trenger et helhetlig tverrsektorielt system for å kunne håndtere dem, og man trenger fleksibilitet.

Hybride trusselaktører angriper motstanderens spesifikke sårbarheter. Disse sårbarhetene vil variere fra situasjon til situasjon, og det samme vil trusselaktørens målsetninger. Derfor er det vanskelig å trekke klare paralleller fra en konflikt til en annen og anta at "lessons learned" vil være direkte overførbare fra et scenario til et annet (Hoffman 2007:7, Galeotti 2016b:1, Renz og Smith 2016:2). Sårbarhetene kan være politiske, militære, økonomiske, sivile, infrastruktur- og informasjonsmessige (Reichborn-Kjennerud og Cullen 2016:2). Oversikt over egne sårbarheter er derfor nødvendig for å vite hva som trenger å forsvares og for å bygge resiliens (Giegerich 2015:14), og i kapittel 3 omtales sårbarhetsanalyser som et viktig supplement for å vurdere en trussel dersom aktøren ikke er kjent. Oversikt over nasjonale sårbarheter og mer globale sårbarheter er sentralt for å identifisere scenarioer der hybride virkemidler kan bli brukt. NSM presenterer nasjonale sårbarheter årlig, og har gjennom mange år konstatert at arbeidet med å rette på disse går for sakte (Elgsaas og Heireng 2014:7). Dette omfatter manglende styring av sikkerhetsarbeid og svakheter innen cyber- og objektsikkerhet, men også hybride trusler og påvirkningsoperasjoner nevnes spesifikt (NSM 2017:8-10). Manglende evne til å følge opp lovpålagte krav er et av elementene som kan lede til en *failure of foresight*. På et overordnet europeisk nivå peker Mölling (2015:17-18) og Fägersten (2016:114) på en rekke sårbarhetsområder som også påvirker Norge. Territoriell integritet i enkelte europeiske land er sårbar på grunn av at europeiske land er militært sett svake. Dette kan åpne for militær opportunisme mot svake småstater, for eksempel i Baltikum. Cyberangrep mot kritisk infrastruktur viser at disse sårbarhetene ikke er avgrenset til det fysiske domenet. Norsk sikkerhetspolitikk legger stor vekt på støtte fra allierte. Politisk samhold i EU og NATO er sårbart på grunn av ulike prioriteringer, der medlemsland i nord og øst er bekymret for Russland, mens land i sør har større fokus på utfordringer rundt Middelhavet. Ekstern støtte til ytterliggående politiske bevegelser, påvirkning av politiske ledere og bestrebelser på å bilateralisere relasjonene til enkeltland vil ytterligere svekke samholdet, og forsinke disse organisasjonenes evne til å treffe raske og effektive beslutninger. Norge er et av de mest digitaliserte landene i verden (JBD 2015:15) Vestlige land er sårbare for avbrudd i global

kommunikasjon og flyt av varer, tjenester, arbeidskraft og kapital. I tillegg finnes det interne sårbarheter i mange land i form av for eksempel økende etniske og religiøse motsetninger og sårbarheter i kritisk infrastruktur (vann, energi, transport, finans og økonomi).

5.2.3 Hybride trusler som "krypende kriser"

Kategorien "krypende kriser" i Boins typologi i kapittel 3 kjennetegnes av at det er utfordrende å si når krisen egentlig starter. Det ligger en fare i at man over tid venner seg til et forhøyet trusselnivå, og det kan bli stadig vanskeligere å "rope ulv" dersom det virker usannsynlig at risikoen skal manifestere seg i en krise. Det er gjerne en politisk beslutning både å erklære at krisen er et faktum og at den er avsluttet. I dette perspektivet handler deteksjon av en koordiner trussel igjen om god situasjonsforståelse og god dialog mellom produsentene av trussel- og risikovurderinger og beslutningstagere. I *sense making*-fasen skapes forståelse av motpartens kapabilitet og intensjon av etterretning fra både åpne og lukkede kilder. Forståelsen påvirkes også av hvor nær trusselen oppfattes i tid og rom. Etter terrorangrepene 22/7 ser det i følge Albrechtsen et. al. (2017) ut som at det er høyere bevissthet i befolkningen og blant aktører på samfunnssikkerhetsområdet om at hendelser med lav sannsynlighet men alvorlige konsekvenser krever spesiell oppmerksomhet. Dette er en positiv utvikling for håndtering av hybride trusler betraktet som "krypende trussel". Siden propaganda og informasjonsoperasjoner er en viktig komponent i en hybrid trussel, vil analyse av åpne kilder (både redigerte og uredigerte media) kunne gi viktig innsikt (msb.se:2009). Det kan være utfordrende å dele graderte etterretninger bredt med private aktører, men det er stadig vanligere at vestlige sikkerhets- og etterretningstjenester publiserer ugraderte nasjonale trussel- og risikovurderinger, noe som ikke minst er viktig for å identifisere relevante trusselscenarioer som kan støtte utviklingen av strategier og systemer for beredskap (Cederberg og Eronen 2015:7) Fra 2017 av skal de ugraderte produktene fra E-tjenesten, NSM, PST og DSB være tydeligere på de enkelte tjenestenes mandat, hva deres vurdering er og hvordan sannsynlighet formidles. Hensikten er blant annet å gjøre det lettere for leserne å sammenligne på tvers av etatene. Deling av etterretninger med allierte vil være sentralt for å forstå det totale omfanget av trusselen. I *decision making*-fasen kommer risikovurderinger på strategisk nivå tydeligere inn. Dyndal (2016:16) stiller spørsmålet om det i det hele tatt er realistisk at en liten stat som Norge vil gå til det steg å offisielt omtale en krise, hendelse eller episode med uten- eller sikkerhetspolitiske

dimensjoner som en "sikkerhetspolitisk krise". Politiske ledere i en småstat vil trolig gå svært langt i å forsøke å løse situasjonen gjennom dialog og diplomati og forsøke å tone den ned så mye som mulig[26], og tjenestenes bidrag vil være viktig for å beskrive kompleksiteten i situasjonen og vurdere motpartens reaksjoner (med de utfordringene som ligger i å vurdere intensjoner).

5.2.4 Befolkningssentrisk trussel

Mark Galeotti (Manea 2016) peker på at et hybrid forsvar til syvende og sist handler om effektiv og legitim styring, som hindrer at desillusjonerte grupper blir stående utenfor storsamfunnet. Korrupsjon og diskriminering av enkeltgrupper med «utenforskap» som resultat skaper sårbarhet. Denne sårbarheten leder til at deler av en befolkning kan bli mer utsatt for radikalisering og ideologisk mobilisering, og har lettere for å tro på konspirasjonsteorier og propaganda som har til hensikt å forsterke motsetninger som allerede eksisterer (Giegerich 2015:14). Norge kan synes mindre sårbart enn mange andre land for slike interne splittelser, men som påpekt av Fermann (2010:55) kan for eksempel endringer i den norske velferdsmodellen som følge av en økonomisk krise lede til negative endringer i både sosial samhørighet og sosial stabilitet. *Stakeholder involvement*-modellen beskriver at behovet for å involvere brede grupper av interessenter øker jo mer komplekse og tvetydige risikoer samfunnet står overfor. Dette representerer et ideal. Jürgen Habermas' tanke om en "opplyst offentlig samtale" er også et ideal som vil bli utfordret av realitetene i uten- og sikkerhetspolitikk: småstaters begrensede handlingsrom, politisk maktkamp, forholdet til både allierte og nabostater som utfordrer vil gjøre dette vanskelig i praksis (Fermann 2010:66). Informasjon og diskusjon om sikkerhetspolitiske realiteter i en normalsituasjon vil i følge Fermann (*ibid.*) sikre at myndighetene har legitimitet og tillit befolkningen dersom en krise skulle oppstå. En befolkningssentrisk hybrid trussel vil bare øke dette behovet.

[26] Denne betraktningen står i sterk kontrast til uttalelsen fra den estiske generalen Riho Terras på spørsmål om hvordan landet ville forholdt seg dersom russiske spesialstyrker dukket opp på estisk territorium: "You should shoot the first one to appear," Gen Terras said. "If somebody without any military insignia commits terrorist attacks in your country you should shoot him ... you should not allow them to enter" (Jones 2015). Mažeikis (2017:11) spør hva som er riktig reaksjon dersom "trusselen" i stedet er representert ved en 15 år gammel jente som deltar i en demonstrasjon.

6. Konklusjon

Problemstillingen la opp til å undersøke hvilke trekk ved hybride trusler som gjør det særlig utfordrende for norske sikkerhetsinstitusjoner å detektere hvorvidt landet er utsatt for en koordinert "kampanje" fra en fremmed stat, eller om hendelsene, alvorlige eller mindre alvorlige, er uten sammenheng. For å operasjonalisere problemstillingen videre, ble to overordnede teoretiske perspektiver benyttet. Det første perspektivet så på sikringstiltak som forutsetninger for deteksjon av en trussel, det andre perspektivet så på trusselbildet, og hybridbegrepets innhold. Under sikringstiltak ble det benyttet teori fra etterretningsstudier, men også bidrag fra safety-området, som *Failure of foresight*, *HRO*). Det har vært et poeng i seg selv å trekke på bidrag fra de to områdene for en mest mulig helhetlig, *all hazards*, tilnærming til stoffet. Den avsluttede drøftingen har vist at safety-teorien inneholder nyttige perspektiver som bidrar til å illustrere problematikken rundt håndtering av hybride trusler på et strategisk nivå. Fenomenet hybride trusler er forsøkt beskrevet med bredt utvalgt sekundær-litteratur, ikke bare fra angloamerikanske kilder som ofte synes å dominere, men også bidrag fra europeiske, spesielt østeuropeiske forskningsmiljøer. Russiske kilder er benyttet for å illustrere at hybridbegrepet i russisk kontekst brukes for å beskrive en trussel fra Vesten mot egen regimestabilitet, men det har ikke vært hensikten å gjøre en komparativ studie av de to oppfatningene, noe som i og for seg kunne vært en interessant studie i seg selv. Et funn som er verd å påpeke er at også på dette området er det ulike oppfatninger av hybride trusler på begge sider av Atlanterhavet, der NATO og europeiske land synes å legge en bredere definisjon til grunn enn det som finnes i amerikanske kilder. Scenario er et nyttig verktøy for å illustrere og diskutere risiko og *wicked problems*. Analysen førte frem til en modell av hybride trusler som viste seg å være hensiktsmessig for å peke ut utfordringer i en norsk kontekst, men den er ikke uttømmende, og det er åpenbart at det finnes andre måter å lage slike modeller på. Fordelen med metoden er at den er transparent og etterprøvbar.

Analysen og drøftingen har identifisert at utfordringen med å vurdere en motstanders intensjoner, og dermed få et mer eller mindre direkte svar på om trusselen er koordinert, er svært utfordrende. Dette krever en egen etterretningsinnsats og samarbeid med allierte som kan gi tidligvarsling, løpende oppdatering og dypere analyser. Men etterretning vil aldri kunne gi sikre svar på dette spørsmålet i alle situasjoner, og derfor er det fornuftig å samtidig "spille forsvar" og satse på at

viktig infrastruktur er godt forsvart mot inntrengning. Sikkerhetstiltak som sårbarhetsvurderinger og informasjonsdeling mellom etater og sektorer vil også være viktig for å sikre at etterretningsfunksjonen fokuserer på det som er relevant til en hver tid. Andre utfordringer som er påvist og drøftet er betydningen av helhetstenkning, fleksibilitet og dynamikk for å møte et trusselbilde som besitter de samme kvalitetene. Ingen krise er lik, og evne til å finne løsninger som fungerer i en krise er avgjørende. Grunnlaget for dette er løpende daglig koordinering mellom etater og sektorer.

Det første forskningsspørsmålet fokuserte på de norske sikkerhetsinstitusjonene, deres ansvarsområder og samarbeidsmåter. Her har det latt seg gjøre å gi en relativt overordnet beskrivelse basert på åpent tilgjengelige kilder. Svaret på det andre spørsmålet er at det finnes åpenbare mangler i nasjonal evne til å detektere enkeltelementer i en hybrid trussel. Dette handler spesielt om evne til å hente inn og analysere data fra det digitale rom, enten for å avdekke fremmed etterretningsvirksomhet eller andre digitale trusler, som planlegging av sabotasje eller påvirkningsoperasjoner. Det finnes heller ikke en god nasjonal evne til å analysere og vurdere påvirkningsoperasjoner rettet mot Norge. Det er identifisert tiltak for å bedre evnen for å detektere digitale trusler, men dette er en debatt som også må ta inn over seg hensyn til personvern. Både myndighetenes og befolkningens persepsjon av trusler vil spille inn i denne debatten. Det tredje spørsmålet handlet om i hvilken grad norske myndigheters persepsjon av trusselen samsvarer med hybride trusler slik de fremkommer i scenarioene. Drøftingen viser at tjenestenes åpne trussel- og risikovurderinger tar for seg de samme typen hendelser som er presentert i scenarioene. Dermed later norske myndigheter til å ha fokus på hybride trusler, selv om forsvarssektoren i mindre grad bruker selve begrepet.

Betyr dette at norske sikkerhetsinstitusjoner og beslutningstagere er i stand til å ”forvente det uventede”? Spørsmålet er filosofisk. Forfatteren mener en slik evne bygges steg for steg basert på erfaringer og forskning. Denne oppgaven har imidlertid pekt på en rekke utfordringer som vil være relevante og identifisert mange steg i retning av å lage et system som kan detektere en eventuell koordinert trussel.

7. Litteraturliste

Albrechtsen, Almklov, Petter Antonsen, Stian Nyheim, Ole Magnus Nilsen, Marie Bye, Rolf Johan Øren, Anita Johnsen, Stig Ole Wasilkiewicz, Kinga Aalberg, Asbjørn (2017) *Har samfunnssikkerheten blitt bedre etter 22. juli 2011?* Rapport fra NTNU [online]. Tilgjengelig fra https://www.safetec.no/wp-content/uploads/2017/11/NEXUS-sluttrapport.pdf. [Lest 2017-11-19].

Andrew, Cristopher., Aldrich, Richard J., og Wark, Wesley K. (2008) *Secret Intelligence - A Reader*. 1 edn. Oxon: Routledge.

Ak-Murza, G. (2014) '*Война глазами добровольцев: ад Иловайска, заминированные игрушки и потребность в ватниках*'. Думская [online], 2014/08/26. Tilgjengelig fra http://dumskaya.net/news/vojna-glazami-dobrovolcev-zaminirovannye-igrushk-038505. [Lest 2017-10-14].

Aldrich, Richard J. (2009) US–European Intelligence Co-operationon Counter-Terrorism: Low Politicsand Compulsion. *The British Journal of Politics and International Relations* Vol 11, ss. 122-129.

Allen & Overy Global Intelligence Unit. (2014) *Ukraine: a brief primer on sanctions, expropriations and state break-ups* [online], London: Allen & Overy. Tilgjengelig fra http://www.allenovery.com/SiteCollectionDocuments/Ukraine%20a%20brief%20primer%20on%20sanctions,%20expropriations%20and%20state%20break-ups.pdf. [Lest 2017-08-16]

Andrews, Cristopher og Mitrokhin, Vasili (1999) *The Sword and the Shield. The Mitrokhin Archive and the Secret History of the KGB*. 1 edn. New York: Basic Books.

Amundrud, Øystein, Aven, Terje og Flage, Roger (2017) How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* [online], 231, (3) ss.286-294. Tilgjengelig fra http://journals.sagepub.com. [Lest 2017-06-23].

Aradau, Claudia, Lobo-Guerrero, Luis og Van Munster, Rens (2008) Security, Technologies of Risk, and the Political: Guest Editor's Introduction. *Security Dialogue* Vol. 39 (2-3), ss. 147-154.

Aven, Terje, og Krohn, Bodil S. (2014) A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and System Safety* [online], 121, (January 2014) ss.1-10. Tilgjengelig fra https://www.journals.elsevier.com. [Lest 2017-06-22]

Aven, Terje (2013) Practical implications of the new risk perspectives. *Reliability Engineering and System Safety* [online], 115 (2013) ss. 136-145. Tilgjengelig fra https://www.journals.elsevier.com. [Lest 2017-06-22].

Aven, Terje og Renn, Ortwin (2010) *Risk Management and Governance: Concepts, Guidelines and Applications*. 2 edn. Heidelberg: Springer.

Aven, Terje (2007) *Risikostyring*. Andre opplag. Oslo: Universitetsforlaget.

Askeland, Tore, Aven, Terje og Flage, Roger (2017) Moving beyond probabilities – strength of knowledge characterizations applied to security. *Reliability Engineering and System Safety* [online], 159, (March) ss.195-205. Tilgjengelig fra http://journals.sagepub.com. [Lest 2017-06-23]

Bachmann, Sascha D. og Munoz Mosquera, Andres B. (2017) Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach. I: Cusumano, Eugenio og Corbe, Marian red. *A Civil-Military Response to Hybrid Threats*. Cham, Sveits: Palgrave Macmillan, ss. 61-76.

Bar-Joseph, Uri. (2005) Intelligence Failure and the Need for Cognitive Closure: The Case of Yom Kippur. I: Betts, Richard K. red. *Paradoxes of Strategic Intelligence - Essays in Honor of Michael I. Handel*. London: Frank Cass Publishers, ss. 159-183.

Beitland, Kristine (2013) *Norske internasjonale selskaper i risikosoner* [online]. Tilgjengelig fra https://www.nsr-org.no/aktuelle-saker/norske-internasjonale-selskaper-i-risikosoner-article288-110.html. [Lest 2017-11-16].

Bjerga, Kjell I. (2010) Forsvarets sentrale ledelse: styring gjennom organisasjon. I: Dyndal, Gjert L. red. *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget, s. 109-129.

Blaikie, Norman. (2010) *Designing Social Research*. 2 edn. Cambridge: Polity.

Boin, Arjen., t' Hart, Paul., Stern, Eric and Sundelius, Bengt (2005) *The Politics of Crisis Management: Public Leadership Under Pressure* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-05].

Bracken, Paul, Bremmer, Ian og Gordon, David red. (2008) *Managing Strategic Surprise: Lessons from Risk Management and Risk Assessment* [kindle]. Tilgjenglig fra https://www.amazon.com. [Lest 2017-04-15].

Bradfield, Ron., Wright, George., Burt, George., Cairns, George., og Van Der Hejden, Kees. (2005) The origins and evolution of scenario techniques in long range business planning. *Futures* [online], 37, ss.795-812. Tilgjengelig fra www.sciencedirect.com. [Lest 2017-07-14].

Bratersky, Alexander (2012). Putin Endorses Eased Citizenship Requirements. *The Moscow Times* [online], 2012-12-12. Tilgjengelig fra https://themoscowtimes.com/articles/putin-endorses-eased-citizenship-requirements-20122. [Lest 2017-10-17].

Buckley, Edgar., Pascu, Ioan. (2015) NATO's Article 5 and Russian Hybrid Warfare. *NATOsource,* [blog] 2015-03-17. Tilgjengelig fra http://www.atlanticcouncil.org/blogs/natosource/nato-s-article-5-and-russian-hybrid-warfare. [Lest 2017-10-17].

Bukkvoll, Tor. (2016) Russian Special operations Forces in the War in Ukraine - Crimea and Donbass. I: Renz, Bettina and Smith, Hanna. red. (2016) *Russia and Hybrid Warfare - Going Beyond the Label* [online], Aleksantari Papers 1/2016. Helsinki: Aleksanteri Institute, ss. 25-33. Tilgjengelig fra http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf. [Lest 2017-08-04]

Busmundrud, Odd., Maal, Maren., Kiran, Jo Hagness og Endregard, Monica (2015) *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* [online], Kjeller: Forsvarets forskningsinstitutt. Tilgjengelig fra https://www.ffi.no/no/Rapporter/15-00923.pdf. [Lest 2017-08-07].

Buzan, Barry., Wæver, Ole og de Wilde, Jaap (1998) *Security – A New Framework for Analysis*. Boulder/London: Lynne Rienner Publishers.

Cavanaugh, Matt L. (2014) *Sun Tzu: Attack the Enemy's Strategy First – Two Recent Examples* [online]. Modern War Institute at West Point. Tilgjengelig fra https://mwi.usma.edu/2014213sun-tzu-attack-the-enemys-strategy-first-two-recent-examples/. [Lest 2017-10-22].

CCDCOE (u.å.) *Cyber Definitions* [online]. NATO Cooperative Cyber Defence Centre of Excellence. Tilgjengelig fra https://ccdcoe.org/cyber-definitions.html. [Lest 2017-07-14].

Chekinov, Sergey G. og Bogdanov, Sergey A. (2010) Асимметричные действия по обеспечению военной безопасности России. *Военная мысль* [online] № 3/2010, ss. 13-22. Tilgjengelig fra http://militaryarticle.ru/voennaya-mysl/2010-vm/10291-asimmetrichnye-dejstvija-po-obespecheniju-voennoj. [Lest 2017-10-28].

Chivvis, Christopher S. (2017) *Understanding Russian "Hybrid Warfare" And What Can Be Done About It* [online], Santa Monica: RAND Corporation. Tilgjengelig fra https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf. [Lest 2017-08-05]

Ciluffo, Frank J., og Clark, Joseph R. (2012) Thinking About Strategic Hybrid Threats — In Theory and in Practice. *PRISM* [online], 4, (1) ss.47-63. Tilgjengelig fra https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/prism4-1.pdf. [Lest 2017-08-05]

Cheng, Dean. (2012) *Winning Without Fighting: Chinese Public Opinion Warfare and the Need for a Robust American Response* [online], Washington, D.C.: The Heritage Foundation. Tilgjengelig fra http://thf_media.s3.amazonaws.com/2012/pdf/bg2745.pdf. [Lest 2017-08-11]

Cederberg, Aapo., Eronen, Pasi. (2015) How Are Societies Defended Against Hybrid Threats? *Strategic Security Analysis* [online], September 2015 No.9: Geneva Center for Security Policy. Tilgjengelig fra http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats. [Lest 2017-08-04].

Clark, Robert M. (2013) *Intelligence Collection*. CQ Press. Thousand Oaks, CA.

Clausewitz, Carl (1873) *On War* [online]. Tilgjengelig fra http://www.clausewitz.com/readings/OnWar1873/TOC.htm#a. [Lest 2017-10-22).

Conley, Heather A. og Stefanov, Ruslan (2016) *The Kremlin Playbook: Understanding Russian In uence in Central and Eastern Europe*. Washington D.C.: Center for Strategic and International Studies.

Covington, Stephen R. (2016) *The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare*. Belfer center for Science and International Affairs [online]. Tilgjengelig fra http://02138www.belfercenter.org/DefenseIntelligence. [Lest 2017-10-06].

Dahl, Arne W. (2008) *Håndbok i militær folkerett*. Andre utgave. Oslo: Cappelen.

Davis, John R. (2015) Continued Evolution of Hybrid Threats. *The Three Swords Magazine* [online], 28, ss.19-25. Tilgjengelig fra http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf. [Lest 2017-08-05].

Dayspring, Stephen M. (2015) *Toward a theory of hybrid warfare: the Russian conduct of war during peace*. Master's thesis. Naval Postgraduate School. Tilgjengelig fra https://calhoun.nps.edu/bitstream/handle/10945/47931/15Dec_Dayspring_Stephen.pdf. [Lest 2017-08-05].

Defence Intelligence Agency/DIA (2017) *Russia Military Power Report 2017* [online]. Washington D.C.: Defence Intelligence Agency. Tilgjengelig fra http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf. [Lest 2017-10-28].

Den russiske ambassade (2017a) *Ambassadens kommentar i forbindelse med NRKs reportasje om Russlands deltakelse i Europarådets arbeid* [online] 2017-10-31. Tilgjengelig fra http://www.norway.mid.ru/press_17_036.html. [Lest 2017-11-15]

Den russiske ambassade (2017b) *Kommentar fra Russlands Ambassade i Norge i forbindelse med foredraget av tidligere norsk generalkonsul i Murmansk av 9. oktober 2017 i Oslo Militære Samfund* [online] 2017-10-20. Tilgjengelig fra http://www.norway.mid.ru/press.html. [Lest 2017-11-15].

Den russiske ambassade (2017c) Vedrørende missilforsvar [online] 2017-01-17. Tilgjengelig fra http://www.norway.mid.ru/press_17_004.html. [Lest 2017-11-15].

Diesen, Sverre (2016) *Forsvarets fremtidige operasjoner - en morfologisk analyse av operasjonsspekteret*. FFI-rapport 16/02096. Kjeller: Forsvarets forskningsinstitutt.

Director of National Intelligence/DNI (2017) *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* [online]. Tilgjengelig fra https://www.dni.gov/files/documents/ICA_2017_01.pdf. [Lest 2017-11-12].

Direktoratet for samfunnssikkerhet og beredskap/DSB (2017) *Totalforsvaret – beredskap for en ny tid?* [online]. Tilgjengelig fra https://www.oslomilsamfund.no/foredrag-totalforsvaret-beredskap-for-en-ny-tid-dsb-cecilie-daae/. [Lest 2017-11-15].

Direktoratet for samfunnssikkerhet og beredskap/DSB (2015) *Departementenes systematiske samfunnssikkerhets- og beredskapsarbeid* [online]. Tilgjengelig fra https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/departementenes-systematiske-samfunnssikkerhetsarbeid.pdf. [Lest 2017-11-14].

Dubovitskiy, Natan (2014) *Без неба*. Русский пионер. [online], 2014-03-12. Tilgjengelig fra http://ruspioner.ru/honest/m/single/4131. [Lest 2017-08-16].

Dunn Cavelty, Myriam., Brunner, Elgin., Giroux, Jennifer., Doktor, Christoph og Brönnimann, Gabriel (2011) Using Scenarios to Assess Risks: Examining Trends in the Public Sector. *CRN Focal Report* 5 [online]. Crisis and Risk Network (CRN), Center for Security Studies (CSS), ETH Zürich. Tilgjengelig fra https://www.academia.edu/attachments/29136071/download_file?st=MTUxMTAyOTIyMSw4NC4yMTEuMjM3LjIyMw%3D%3D&s=swp-splash-paper-cover. [Lest 2017-11-16].

Dunn Cavelty, Myriam, og Mauer, Victor (2009) Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence. *Security Dialogue* [online], 40, (2) ss.123-144. Tilgjengelig fra http://journals.sagepub.com. [Lest 2017-08-05].

Dyndal, Gjert L. red. (2010) *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget.

Elgsaas, Ingvill M. og Heireng, Hege S. (2014) *Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet*. FFI-rapport 2014/00948. Kjeller: Forsvarets forskningsinstitutt.

Eschevarria, Antulio J. (2016) How Should We Think About "Gray-Zone" Wars? I: Renz, Bettina and Smith, Hanna. red. (2016) *Russia and Hybrid Warfare - Going Beyond the Label* [online], Aleksantari Papers 1/2016. Helsinki: Aleksanteri Institute, ss. 33-39. Tilgjengelig fra http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf. [Lest 2017-11-14]

European Union External Action Service/EEAS (2017). *Questions and Answers about the East StratCom Task Force* [online]. Tilgjengelig fra https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/%20Questions%20and%20Answers%20about%20the%20East%20StratCom%20Task%20Force. [Lest 2017-11-15].

Feaver, Peter (2010) Defining Diplomacy, *Foreign Policy* [online] 2010-04-01. Tilgjengelig fra http://foreignpolicy.com/2010/04/01/defining-diplomacy/. [Lest 2017-11-20).

Fermann, Gunnar (2010). Strategisk ledelse i et utenrikspolitisk perspektiv. I: Dyndal, Gjert L. red. *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget, ss. 25-75.

Fimreite, Anne L., Lægreid, Per og Rykkja, Lise H. (2011) *Organisering, samfunnssikkerhet og krisehåndtering*. Oslo: Universitetsforlaget.

Flakstad, Patricia (2010) Forsvarets strategiske krisehåndteringsapparat. I: Dyndal, Gjert L. red. *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget, s. 109-129.

Foley, Frank (2011) *Countering Terrorism in Britain and France: Institutions, Norms and the Shadow of the Past* [kindle]. Tilgjengelig fra www.amazon.com. [Lest 2017-10-29].

Foley, Frank (2009) Reforming Counterterrorism: Institutions and Organizational Routines in Britain and France. *Security Studies* 18, ss. 435-478.

Forskningsrådet (2006) *Få muligheter til å sikre investeringer i Russland* [online], Tilgjengelig fra https://www.forskningsradet.no/no/Nyheter/Fa+muligheter+til+a+sikre+investeringer+i+Russland/1236685426105. [Lest 2017-10-17].

Forsvarsdepartementet/FD (2017a) *Lov om nasjonal sikkerhet (sikkerhetsloven)*. Prop. 153 L (2016-2017). Oslo: Forsvarsdepartementet.

Forsvarsdepartementet/FD (2017b) *Statusrapport. Landmaktutredningen, juni 2017*. Oslo: Forsvarsdepartementet.

Forsvarsdepartementet/FD (2016a) *Kampkraft og bærekraft. Langtidsplan for forsvarssektoren.* Prop. 151 S (2015–2016). Oslo: Forsvarsdepartementet.

Forsvarsdepartementet/FD (2016b) *Et Forsvar for vår tid*. Prop. 73 S (2011–2012). Oslo: Forsvarsdepartementet.

Forsvarsdepartementet/FD (2016c) *Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* NOU 2016:19. Oslo: Forsvarsdepartementet.

Forsvarsdepartementet/FD (2016d) *En god alliert – Norge i Afghanistan 2001–2014.* NOU 2016:8. Oslo: Forsvarsdepartementet.

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

Forsvarsdepartementet/FD (2015b) *Et felles løft*. (Ekspertgruppen for Forsvaret av Norge). Oslo: Forsvarsdepartementet.

Forsvaret (2017) *Forsvarets operative hovedkvarter* [online]. Tilgjengelig fra https://forsvaret.no/foh. [Lest 2017-11-15].

Forsvarssjefen/FSJ (2015) *Et forsvar i endring. Forsvarssjefens fagmilitære råd* [online]. Tilgjengelig fra https://forsvaret.no/fakta_/ForsvaretDocuments/EtForsvariEndring-Nett.pdf. [Lest 2017-11-15].

Fägersten, Bjørn (2017) Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence I: Hamilton, Daniel S. red. *Forward Resilience: Protecting Society in an Interconnected World* [online], Center for Transatlantic Relations. Tilgjengelig fra http://transatlanticrelations.org/topic/security-and-resilience/forward-resilience-protecting-society-interconnected-world/. [Lest 2017-10-20].

Galeotti, Mark (2017) *Russian intelligence is at (political) war* [online], Tilgjengelig fra http://www.nato.int/docu/review/2017/Also-in-2017/russian-intelligence-political-war-security/EN/index.htm. [Lest 2017-08-14].

Galeotti, Mark (2016a) *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear militrary challenge right*. Mayak Intelligence.

Galeotti, Mark (2016b) Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war? *Small Wars & Insurgencies* [online] 22, (2) ss. 282-301. Tilgjengelig fra Taylor & Francis Online: http://dx.doi.org/10.1080/09592318.2015.1129170. [Lest 2017-10-14]

Galvach, Zane M., Mesko, Matthew J., Everett, Thomas B., Dickey, Jeffrey V. og Soltis, Anton V. (2015) *Russian Political Warfare: Origin, Evolution and Application* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-16].

Gentry, John A. (2017) The Intelligence of Fear. *Intelligence and National Security*. 2017, Vol. 32, No. 1 ss. 9-25.

Gerasimov, Valeriy (2017). Мир на гранях войны. *Военно-промышленный курьер* [online] 10, (674). Tilgjengelig fra http://vpk-news.ru/articles/35591. [Lest 2017-08-04]

Gerasimov, Valeriy (2013) Ценность науки в предвидении. *Военно-промышленный курьер* [online] 8, (476). Tilgjengelig fra http://www.vpk-news.ru/articles/14632. [Lest 2017-08-16].

Giegerich, Bastian (2016) Hybrid Warfare and the Changing Character of Conflict. *Connections: The Quarterly Journal* [online] 15, (2) ss.65-72. Tilgjengelig fra https://connections-qj.org/system/files/15.2.05_giegerich_hybrid_warfare.pdf. [Lest 2017-07-23].

Giegerich, Bastian (2015) Hybrid Attacks Demand Comprehensive Defense. *Ethics and Armed Forces* [online] 2015/2. Tilgjengelig fra http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/giegerich-hybrid-attacks-demand-comprehensive-defense. [Lest 2017-08-05].

Giles, Keir (2016) *Russia's 'New' Tools for Confronting the West. Continuity and Innovation in Moscow's Exercise of Power* [online], London: Chatham House. Tilgjengelig fra http://https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf. [Lest 2017-08-05].

Gill, Peter (2010) Theories of Intelligence. In Johnson, Loch K. red. (2010) *The Oxford Handbook of National Security Intelligence*. Reprint edition. New York: Oxford University Press.

Grabo, Cynthia M. (2002) *Anticipating Surprise: Analysis for Strategic Warning.* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-22].

Grau, Lester (1990) *Soviet Non-Linear Combat: The Challenge of the 90s* [online] Fort Leavenworth: U.S. Army Combined Arms Center. Tilgjengelig fra http://www.dtic.mil/dtic/tr/fulltext/u2/a231789.pdf. [Lest 2017-08-17].

Grigas, Agnia (2016) *Separatists Launch New "Passportization" Strategy in Eastern Ukraine* [online], Tilgjengelig fra http://www.atlanticcouncil.org/blogs/ukrainealert/separatists-launch-new-passportization-strategy-in-eastern-ukraine. [Lest 2017-08-15].

Gusarov, Vyacheslav (2016) *Особенности организации и ведения радиоэлектронной борьбы в боях за Иловайск. Аналитика ИС* [online], Tilgjengelig fra http://sprotyv.info/ru/news/kiev/osobennosti-organizacii-i-vedeniya-radioelektronnoy-borby-v-boyah-za-ilovaysk-analitika. [Lest 2017-10-14].

Hagen, Guro Aa. (2009) *Slik fungerer russisk rett*. Dagens næringsliv [online], Tilgjengelig fra https://www.dn.no/tekno/2009/09/30/slik-fungerer-russisk-rett. [Lest 2017-10-17].

Hagen, Janne M. og Søgaard, Henning A. (2013) *Strategisk kommunikasjon som redskap i krisehåndtering*. FFI-rapport 2013/03101 [online], Kjeller: Forsvarets forskningsinstitutt. Tilgjengelig fra http://https://www.ffi.no/no/Rapporter/13-03101.pdf. [Lest 2017-08-04].

Hagen, Janne M., Knutsen, Bjørn. O., Bjørnenak, Morten og Sandrup, Terese (2011) *Scenarioer for samfunnssikkerhet og nasjonal beredskap*. FFI-rapport 2011/00648 [online], Kjeller: Forsvarets forskningsinstitutt. Tilgjengelig fra https://www.ffi.no/no/Rapporter/11-00648-2.pdf. [Lest 2017-10-22].

Halper, Stefan (2013) Executive Summary, in Halper, Stefan. red. (2013) *China: The Three Warfares* [online], Washington, D.C.: Office of the Secretary for Defense, ss. 11-21. Tilgjengelig fra https://cryptome.org/2014/06/prc-three-wars.pdf. [Lest 2017-07-30].

Hamilton, Daniel S. (2017) Going beyond Static Understandings: Resilience Must Be Shared, and It Must Be Projected Forward. I: Hamilton, Daniel S. red. *Forward Resilience: Protecting*

Society in an Interconnected World [online], Center for Transatlantic Relations. Tilgjengelig fra http://transatlanticrelations.org/topic/security-and-resilience/forward-resilience-protecting-society-interconnected-world/. [Lest 2017-10-20].

Handel, Michael I. (2005) Intelligence and the Problem of Strategic Surprise, I: Betts, Richard K. and Mahnken, Thomas G. red. (2005) *Paradoxes of Strategic Intelligence - Essays in Honor of Michael I. Handel.* London: Frank Cass Publishers, ss. 1-57.

Hatch, Scott J. (2013) Managing the "Reliability Cycle": An Alternative Approach to Thinking About Intelligence Failure. *Studies in Intelligence* [online] 57, (2) ss.29-37. Tilgjengelig fra https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-57-no-2/pdfs/Hatch-Reliability%20Cycle.pdf. [Lest 2017-08-04].

Hatlebrekke, Kjetil A, og Smith, M. L. R. (2010) Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure. *Intelligence and National Security* [online] 25, (2) ss.147-182. Tilgjengelig fra http://www.tandfonline.com. [Lest 2017-08-04].

Hoffman, Francis G. (2017) *The Evolution of Hybrid Warfare and Key Challenges* [online], Washington D.C.: House Armed Services Committee. Tilgjengelig fra https://armedservices.house.gov/legislation/hearings/full-committee-hearing-evolution-hybrid-warfare-and-key-challenges. [Lest 2017-08-16].

Hoffman, Frank (2014) On Not-So-New Warfare: Political Warfare vs Hybrid Threats, *War on the Rocks*. [Blog] 2014-07-28. Tilgjengelig fra https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats. [Lest 2017-08-03].

Hoffman, Frank (2007) *Conflict in the 21st Century: The Rise of Hybrid Wars* [online], Potomac Institute for Policy Studies: Tilgjengelig fra http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. [Lest 2007-08-04].

Hulnick, Arthur S. (2005) Indications and Warning for Homeland Security: Seeking a New Paradigm. *International Journal of Intelligence and Counter Intelligence* 18 (4), ss. 593-608.

Høgskolen i Bergen (2015) *Multimediejournalistikk* (nettstudium) [online], Tilgjengelig fra https://sites.google.com/site/multimediejournalistikk/home. [Lest 2017-10-14].

International Institute for Strategic Studies/IISS (2014) Countering hybrid threats: challenges for the West. *Strategic Comments* [online], 20, (8). Tilgjengelig fra http://www.tandfonline.com. [Lest 2017-08-05]

Jackson, L. (2015) The Three Warfares—China's New Way of War, in Pomerantsev, Peter. red. (2015) *Information at War: From China's Three Warfares to NATO's Narratives* [online], London: Legatum Institute, ss. 5-16. Tilgjengelig fra http://stratcomcoe.org/download/file/fid/1504. [Lest 2017-10-13].

Jacobsen, Dag I. (2015) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. 3 edn. Oslo: Cappelen Damm.

Jagello 2000 (2016) *Hybrid warfare: A new phenomenon in Europe's security environment*. Updated and extended 2nd edition [online]. Praha/Ostrava: Jagello 2000 for NATO Information Centre in Prague. Tilgjengelig fra http://data.idnes.cz/soubory/na_knihovna/A161212_M02_029_HH16_PP-EN-V1.PDF. [Lest 2017-11-19].

Johansen, Iver. (2014) *En morfologisk analyse av scenarioklasser for norske spesialstyrker – metode og tilnærming* [online], Kjeller: Forsvarets forskningsinstitutt. Tilgjengelig fra http://https://www.academia.edu/26773381/En_morfologisk_analyse_av_scenarioklasser_for_norske_spesialstyrker_metode_og_tilnaerming?auto=download. [Lest 2017-08-05].

Johansen, Iver. (2006) *Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge* [online], Kjeller: Forsvarets forskningsinstitutt. Tilgjengelig fra http://http://www.ffi.no/no/Rapporter/06-02664.pdf. [Lest 2017-08-05].

Jones, Sam (2015) Estonia ready to deal with Russia's 'little green men'. *Financial Times* [online] 2015-05-13. Tilgjengelig fra https://www.ft.com/content/03c5ebde-f95a-11e4-ae65-00144feab7de. [Lest 2017-11-15].

Jore, Sissel H. og Egeli, Anne. (2015) Risk management methodology for protecting against malicious acts - are probabilities adequate means for describing terrorism and other security risks? I: Podofillini, Luca. red. *Safety and Reliability of Complex Engineered Systems*. London: Taylor Francis, ss. 807-815.

Jore, Sissel H. (2012) *Counterterrorism as Risk Management Strategies*. Phd. Thesis. Universitetet i Stavanger.

Justis- og beredskapsdepartementet/JBD (2016) *Risiko i et trygt samfunn — Samfunnssikkerhet*. Meld. St. 10 (2016–2017). Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet/JBD (2015) *Digital sårbarhet – sikkert samfunn*. NOU 2015:13. Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet/JBD (2012) *Ekstern gjennomgang av Politiets sikkerhetstjeneste - Rapport fra Traavikutvalget*. Oslo: Justis- og beredskapsdepartementet.

Justis- og politidepartementet/JPD (2002) *Samfunnssikkerhet*. St.meld. nr. 17 (2001-2002). Oslo: Justis- og politidepartementet.

Karber, Phillip A (2015) *Russia's 'New Generation Warfare'* [online], Tilgjengelig fra https://www.nga.mil/MediaRoom/News/Pages/Russia%27s-%27New-Generation-Warfare%27.aspx. [Lest 2017-08-16].

Kaitsepolitseiamet (Kapo). (2016) *Annual Review* [online], Tallin: Estonian Internal Security Service. Tilgjengelig fra https://www.kapo.ee/sites/default/files/public/content_page/Annual%20Review%202016.pdf. [Lest 2017-08-20].

Karlsen, Geir H. (2010) *Hybridkrig – militærteoriens Janusansikt?* [online], Master Dissertation. Oslo: Forsvarets stabsskole. Tilgjengelig fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/99898/Karlsen%2C%20Geir.pdf?sequence=1. [Lest 2016-08-16].

Kennan, George F. (1948) *The inauguration of organized political warfare* [online], Wilson Center Digital Archive: Wilson Center. Tilgjengelig fra http://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c. [Lest 2017-08-04].

Klus, Adam. (2016) Myatezh Voina: The Russian Grandfather of Western Hybrid Warfare. *Small Wars Journal.* [Blog] 2016-07-10. Tilgjengelig fra http://smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare. [Lest 2017-08-02].

Knight, Ken (2006) *A Practitioner's View of Emerging Challenges for Warning* [online], Zurich: Center for Security Studies, ETH Zurich. Tilgjengelig fra https://www.files.ethz.ch/isn/28419/EmergingThreatsInThe21stCentury.pdf. [Lest 2017-08-05].

Knutsen, Torbjørn L. (2010) Om militær makt og myndighet. I: Dyndal, Gjert L. red. *Strategisk ledelse i krise og krig*. Bergen: Fagbokforlaget, s. 363-375.

Kofman, Michael (2016) Russian Hybrid Warfare and Other Dark Arts, *War on the Rocks*, [blog] 2016-03-11, tilgjengelig fra https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts. [Lest 2017-05-25].

Kofman, Michael og Rojanski, Matthew (2015) A Closer Look at Russia´s "Hybrid War" [online], *Kennan Cable* (No. 7), tilgjengelig fra https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf. [Lest 2017-05-11].

Kosow, Hannah og Gaßner, Robert (2008) *Methods of Future and Scenario Analysis: Overview, Assessment and Selection Criteria* [online]. Tilgjengelig fra https://www.die-gdi.de/uploads/media/Studies_39.2008.pdf. [Lest 2017-11-17].

Kragh, Martin og Åsberg, Sebastian (2017). Russia's strategy for influence through public diplomacy and active measures: the Swedish case. *Journal of Strategic Studies* [online], ss.1-44. Tilgjengelig fra http://dx.doi.org/10.1080/01402390.2016.1273830. [Lest 2017-08-07].

Krekó, Péter., Györi, Lóránt og Zgut, Edit (2017) *From Russia With Hate: The activity of pro-Russian extremist groups in Central-Eastern Europe* [online]. Tilgjengelig fra http://www.politicalcapital.hu/news.php?article_read=1&article_id=933. [Lest 2017-11-15].

Kristoffersen, Lene (2006) *Sivilt-militært samarbeid (CIMIC)*[online]. Den norske Atlanterhavskomité. Tilgjengelig fra http://www.atlanterhavskomiteen.no/files/atlanterhavskomiteen.no/Publikasjoner/KortInfo/Arkiv/2006/kortinfofinal%202-2006.pdf. [Lest 2017-10-21].

Kruke, Bjørn I. (2012) *Samfunnssikkerhet og krisehåndtering: relevans for 22. juli 2011* [online], Oslo: 22. juli-kommisjonen. Tilgjengelig fra https://www.regjeringen.no/html/smk/22julikommisjonen/22JULIKOMMISJONEN_NO/CONTENT/DOWNLOAD/216/1700/VERSION/1/FILE/NOTAT_7_KRUKE___SAMFUNNSSIKKERH.PDF. [Lest 2017-07-23].

Kruke, Bjørn I., Olsen, Odd E., Hovden, Jan (2005) *Samfunnssikkerhet – forsøk på en begrepsfesting*. Notat 2005/034. Stavanger: Rogalandsforskning.

Kuhns, Woodrow J. (2005) Intelligence Failures: Forecasting and the Lessons of Epistemology, in Betts, Richard K. and Mahnken Thomas G. red. (2005) *Paradoxes of Strategic Intelligence - Essays in Honor of Michael I. Handel*. London: Frank Cass Publishers, ss. 77-97.

Kvamme, Pål (2017) – Ikke interessert i hvem som står bak. *AldriMer.no* [online], 2017-04-28. Tilgjengelig fra https://www.aldrimer.no/ikke-interessert-i-hvem-som-star-bak/. [Lest 2017-11-16].

Lasconjarias, G., og Larsen, J. red. (2015) *NATO's Response to Hybrid Threats* [online], NATO Defense College. Tilgjengelig fra http://https://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjKoJu-p_PWAhXkK5oKHTwJD6IQFggsMAA&url=http%3A%2F%2Fwww.ndc.nato.int%2Fdownload%2Fdownloads.php%3Ficode%3D471&usg=AOvVaw0iCd8XF93eLrTBsv_220gL. [Lest 2017-10-14].

Lindén, Lars (2015) *Sikkerhetsrådgivning: Norske myndigheters sikkerhetsrådgivning overfor store norske bedrifter med virksomhet i utlandet* [online], Masteroppgave. Politihøgskolen. Tilgjengelig fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/284512/master_Linden_2015.pdf?sequence=1. [Lest 2017-11-17].

Lowenthal, Mark M. (2015) *Intelligence: From Secrets to Policy*. 6 edn. CQ Press, Thousand Oaks, CA.

Lysne II-utvalget (2016) *Digitalt grenseforsvar (DGF)* [online]. Tilgjengelig fra https://www.regjeringen.no/contentassets/ca1f705dbebd48cb9a61889d4cfee6bf/digitalt-grenseforsvar-lysne-ii-utvalget.pdf. [Lest 2017-11-11].

Manea, Octavian (2015) Hybrid War as a War on Governance: Interview by Octavian Manea with Dr. Mark Galeotti, *Small Wars Journal* [blog], 2015-08-19, tilgjengelig fra http://smallwarsjournal.com/jrnl/art/hybrid-war-as-a-war-on-governance. [Lest 2017-05-25].

Martins, J., Santos, H., Nunes, P., & Silva, R. (2012b). *Information Security Model to Military Organizations in Environment of Information Warfare*. Paper presented at the 11 th European Conference on Information Warfare and Security, Laval, France. Tilgjengelig fra https://www.researchgate.net/publication/233981496_Information_Security_Model_to_Military_Organizations_in_Environment_of_Information_Warfare. [Lest 2017-04-12].

Masters, Jonathan (2017) *What Are Economic Sanctions?* [online], tilgjengelig fra https://www.cfr.org/backgrounder/what-are-economic-sanctions. [Lest 2017-08-15].

Mattilsynet (2017) Økt sikkerhet og beredskap i vannforsyningen - fra ROS til operativ beredskap [online]. Tilgjengelig fra https://www.mattilsynet.no/mat_og_vann/vann/vannforsyningssystem/okt_sikkerhet_og_beredskap_i_vannforsyningen__fra_ros_til_operativ_beredskap. [Lest 2017-11-15].

Mattis, James N. og Hoffman, Frank (2005) 'Future Warfare: The Rise of Hybrid Wars'. *Proceedings Magazine* [online], 132, tilgjengelig fra http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf. [Lest 2017-07-03].

Maurer, Tim (2015) Cyber Proxies and the Crisis in Ukraine. I: Geers, Kenneth red. (2015) *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence, ss. 79-87.

Mazarr, Michael J. (2016) *Rethinking Risk in National Security: Lessons of the Financial Crisis for Risk Management* [kindle] Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-08].

Mazarr, Michael J. (2015) *Mastering the Gray Zon: Understanding a Changing Era of Conflict* [online], Carlisle, PA: U.S. Army War College. Tilgjengelig fra http://https://ssi.armywarcollege.edu/pdffiles/PUB1303.pdf. [Lest 2017-08-08].

Mažeikis, Edvardas (2017) Keynote Speech. *Energy Security forum* 11 [online], NATO Energy Security Forum Centre of Excellence, ss. 5-8. Tilgjengelig fra https://enseccoe.org/data/public/uploads/2017/03/zurnalas_no11_sp_176x250mm_3mm_2.pdf. [Lest 2017-07-03].

McCarthy, Shaun P. (1998) *The Function of Intelligence in Crisis Management – Towards an understanding of the intelligence producer-consumer dichotomy*. Aldershot: Ashgate Publishing Company.

McDermott, Roger N. (2017) *Russia's Electronic Warfare Capabilities to 2025. Challenging NATO in the Electromagnetic Spectrum* [online], Tallinn: International Centre for Defence and Security. Tilgjengelig fra

https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf. [Lest 2017-10-14].

Messner, Evgeniy E. (2005) *Хочешь мира, победи мятежевойну!* [online], Москва: Военный Университет / Русский путь. Tilgjengelig fra http://http://militera.lib.ru/science/0/pdf/messner_ea01.pdf. [Lest 2017-08-04].

Meyer-Minnemann, Lorenz (2017) Resilience and Alliance Security: The Warsaw Commitment to Enhance Resilience. I: Hamilton, Daniel S. red. *Forward Resilience: Protecting Society in an Interconnected World* [online], Center for Transatlantic Relations. Tilgjengelig fra http://transatlanticrelations.org/topic/security-and-resilience/forward-resilience-protecting-society-interconnected-world/. [Lest 2017-10-20].

Ministerstvo Vnitra České Republiky/MVČR (2017) *Centre Against Terrorism and Hybrid Threats* [online]. Tilgjengelig fra http://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx. [Lest 2017-11-15].

Mitrokhin, Vasili (2013) *KGB Lexicon: The Soviet Intelligence Officers Handbook* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-11].

Moore, John. (2017) Lawfare. *Three Swords Magazine* [online] 31, ss.38-43. Tilgjengelig fra http://www.jwc.nato.int/images/stories/_news_items_/2017/Lawfare_Moore.pdf. [Lest 2017-08-20].

Murphy, Martin N. (2012) Deep-Water Oil Rigs as Strategic Weapons, *New Atlanticist*. [Blog] 2012-09-19. Tilgjengelig fra http://www.atlanticcouncil.org/blogs/new-atlanticist/deepwater-oil-rigs-as-strategic-weapons. [Lest 2018-08-20].

Murray, W. og Mansoor, P. R. red. (2012) *Hybrid warfare: Fighting Complex Opponents from the Ancient World to the Present* [kindle] Tilgjengelig fra https://www.amazon.com. [Lest 2017-10-14].

Myasnikov, Viktor (2005) Конец противоборства по Клаузевицу. *Независимое Военное Обозрение*. [online] 2005-07-09. Tilgjengelig fra http://nvo.ng.ru/concepts/2005-07-08/4_messner.html. [Lest 2017-08-04].

Myndigheten för samhällsskydd och beredskap/MSB (u.å.) *Psykologiskt försvar* [online] Tilgjengelig fra https://www.msb.se/sv/Insats--beredskap/Psykologiskt-forsvar. [Lest 2017-08-15].

Mölling, Christian. (2015) From Hybrid Threats to Hybrid Security Policy. *Ethics and Armed Forces* [online] 2015/2, ss.. Tilgjengelig fra http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/moelling-from-hybrid-threats-to-hybrid-security-policy. [Lest 2017-08-05].

Nasjonal kommunikasjonsmyndighet/Nkom (2017) *EkomROS 2017 – Risikovurdering av ekomsektoren* [online]. Tilgjengelig fra https://www.nkom.no/aktuelt/rapporter/_attachment/29084?_ts=15c9b3cff27. [Lest 2017-11-17].

Nasjonal kommunikasjonsmyndighet/Nkom (2016) *EkomROS 2016 – Risikovurdering av ekomsektoren* [online]. Tilgjengelig fra https://www.nkom.no/aktuelt/rapporter/_attachment/23586?_ts=1545b7b03d0. [Lest 2017-11-17].

Nasjonal Sikkerhetsmyndighet/NSM (2017) *Risiko og sårbarheter i en ny tid*. Oslo: Nasjonal Sikkerhetsmyndighet.

Nasjonal Sikkerhetsmyndighet/NSM (2014a) *Dette gjør NSM* [online]. Tilgjengelig fra https://nsm.stat.no/om-nsm/tjenester/. [Lest 2017-11-11].

Nasjonal Sikkerhetsmyndighet /NSM (2014b) *Varslingssystem for digital infrastruktur (VDI)* [online]. Tilgjengelig fra https://nsm.stat.no/norcert/varslingssystem-for-digital-infrastruktur-vdi/. [Lest 2017-11-11].

Nathan, Patrick. (2006) *A Practitioner's View of Emerging Challenges for Warning* [online] Zurich: Center for Security Studies, ETH Zurich. Tilgjengelig fra https://www.files.ethz.ch/isn/28419/EmergingThreatsInThe21stCentury.pdf. [Lest 2017-08-05]

National Commission on Terrorist Attacks upon the United States (9/11 Commission), Thomas H. Kean, og Lee Hamilton. (2004) *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. Washington D.C.

NATO (2014) *Wales Summit Declaration* [online]. Tilgjengelig fra https://www.nato.int/cps/ic/natohq/official_texts_112964.htm. [Lest 2017-06-24].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE u.å.) *Cyber Definitions* [online] Tilgjengelig fra https://ccdcoe.org/cyber-definitions.html. [Lest 2017-08-22].

Neville, S. B. (2015) *Russia and Hybrid Warfare: Identifying Critical Elements in Successful Applications of Hybrid Tactics - Putin's Crimea Annexation, Ukraine, 1923 German Revolution, Germany's Austria Annexation* [kindle] Tilgjengelig fra https://www.amazon.com. [Lest 2017-10-14].

NITO (2017) *Usikkerhet med ny sikkerhetslov* [online]. Tilgjengelig fra https://www.nito.no/aktuelt/2017/6/usikkert-med-ny-sikkerhetslov/. [Lest 2017-11-11].

Organization for Economic Co-operation and Development/OECD (2003) *Emerging Systemic Risks in the 21st Century: An Agenda for Action* [online]. Tilgjengelig fra https://www.oecd.org/futures/globalprospects/37944611.pdf. [Lest 2017-11-12].

Oliphant, Roland og McGoogan, Cara (2017) Nato warns cyber attacks 'could trigger Article 5' as world reels from Ukraine hack. *The Telegraph* [online] 2017-06-28. Tilgjengelig fra http://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples/. [Lest 2017-07-15].

Olsen, Odd E., Reiss Mathiesen, Espen og Boyesen, Marit (2008) *Media og krisehåndtering: En bok om samspillet mellom media og krisehåndterere*. Kristiansand: Høyskoleforlaget.

Olsen, Odd E., Kruke, Bjørn I. Og Hovden, Jan (2007) Social Safety: Concept, Borders and Dilemmas. *Journal of Contingencies and Crisis Management* Volume 15, number 2, June 2007, ss. 69-79.

Omand, David (2015) *Securing The State* [kindle] Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-09].

Orekh", Anton (2008) Паспорт как бацилла. *Ежедневный Журнал*. [online] 2008-09-09. Tilgjengelig fra http://www.ej.ru/?a=note&id=8381. [Lest 2017-08-15].

Pawlak, Patryk (2017) *Countering hybrid threats: EU-NATO cooperation* [online] Brussels: European Parliamentary Research Service. Tilgjengelig fra http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf. [Lest 2017-08-05].

Perepelitsya, Grigoriy M. (2015) *Україна – Росія: війна в умовах співіснування.* Київ: Видавничий дім "Стилос".

Perrow, Charles (2011) *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* [kindle]. Tilgjengelig fra www.amazon.com. [Lest 2017-11-10].

Perrow, Charles (2006) The Disaster after 9/11: The Department of Homeland Security and the Intelligence Reorganization. *Homeland Security Affairs* 2, Article 3 (April 2006). Tilgjengelig fra https://www.hsaj.org/articles/174. [Lest 2017-11-12].

Perrow, Charles (1999) *Normal Accidents: Living with High-Risk Technologies*. 2 edn. Princeton: Princeton University Press.

Petersen, Karen L. (2017) Risk and Security. I: Dunn Cavelty, Myriam og Balzacq, Thierry (2017) *Routledge Handbook of Security Studies* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-08-01].

Petersen, Karen L. og Tjalve, Vibeke S. (2017) Intelligence expertise in the age of information sharing: public–private 'collection' and its challenges to democratic control and accountability. *Intelligence and National Security* [online], ss. 1-15. Tilgjengelig fra http://www.tandfonline.com/doi/full/10.1080/02684527.2017.1316956. [Lest 2017-09-05].

Petersen, Karen L. og Tjalve, Vibeke S. (2012) 21st Century Risk and Security Governance: Neo-liberal, Neorepublican, or …? *Risk and Regulation*, No. 23 Summer 2012 [online]. Tilgjengelig fra https://issuu.com/carr/docs/rr23_summer_2012. [Lest 2017-09-05].

Pidgeon, Nick F. (2010) 'Systems thinking, culture of reliability and safety'. *Civil Engineering and Environmental Systems* [online] 27, (3) ss.211-217. Tilgjengelig fra http://www.icesi.edu.co/blogs/pslunes122/files/2012/08/Systems-thinking-culture-of-reliability-and-safety1.pdf. [Lest 2017-08-05].

Pièrre-Cambacédès, Ludovic., og Chaudet, Claude (2013) 'Cross-fertilization between safety and security engineering'. *Reliability Engineering and System Safety* [online] 110, (2013) ss.110-126. Tilgjengelig fra https://www.researchgate.net/publication/257392110_Cross-fertilization_between_safety_and_security_engineering. [Lest 2017-08-05].

Plekhanov, Il'ya (2017) *"Доктрина Герасимова" и пугало "гибридной войны" России*. РИА Новости. [online] 28/06. Tilgjengelig fra https://ria.ru/analytics/20170628/1497445931.html. [Lest 2017-08-04].

Politidirektoratet (2014) *Etterretningsdoktrine for Politiet* [online]. Oslo: Politidirektoratet. Tilgjengelig fra https://www.politi.no/globalassets/dokumenter/03-strategier-og-planer/etterretningsdoktrine.pdf. [Lest 2017-10-31].

Politiets sikkerhetstjeneste/PST (2017) *Trusselvurdering 2017* [online]. Tilgjengelig fra http://www.pst.no/media/82648/pst_trusselvurd_2017_no_web.pdf. [Lest 2011-11-11].

Politiets sikkerhetstjeneste/PST (2016) *Trusselvurdering 2016* [online]. Tilgjengelig fra http://www.pst.no/media/81096/PST_Brosjyre_Trussel_NORSK.pdf. [Lest 2011-10-01].

Politiets sikkerhetstjeneste/PST (2011) *Trusselvurdering 2011* [online]. Tilgjengelig fra http://www.pst.no/media/utgivelser/trusselvurdering-2011/. [Lest 2011-11-11].

Politiets sikkerhetstjeneste/PST (u.å.) *Oppgaver* [online]. Tilgjengelig fra http://www.pst.no/oppgaver/. [Lest 2017-11-11].

Politiets sikkerhetstjeneste/PST (u.å.) *Samarbeid* [online]. Tilgjengelig fra http://www.pst.no/oppgaver/samarbeid/. [Lest 2017-11-14].

Pomerantsev, Peter (2014) *How Putin Is Reinventing Warfare*. Foreign Policy. [online] 05 May. Tilgjengelig fra http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare. [Lest 2017-08-16].

Pomerantsev, Peter (2014) Non-Linear War, *London Review of Books blog*. [Blog] 2014-03-28. Tilgjengelig fra https://www.lrb.co.uk/blog/2014/03/28/peter-pomerantsev/non-linear-war. [Lest 2017-08-16].

Postma, Theo J B M. og Liebl, Franz (2005) 'How to improve scenario analysis as a strategic management tool'. *Technological Forecatsing and Social Change* [online] 72, (2005) ss.161-173. Tilgjengelig fra www.sciencedirect.com. [Lest 2017-08-05].

Prezident Rossii (2014) *Подписаны законы о принятии Крыма и Севастополя в состав Россиии* [online], Tilgjengelig fra http://kremlin.ru/events/president/news/20625. [Lest 2017-10-17].

Qiao, Liang, og Wang, Xiangsui (1999) *Unrestricted Warfare* [online], Beijing: PLA Literature and Arts Publishing House. Tilgjengelig fra http://https://ia800201.us.archive.org/0/items/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui.pdf. [Lest 2017-08-16].

Radin, Andrew (2017) *Hybrid Warfare in the Baltics - Threats and Potential Responses* [online], Santa Monica: RAND Corporation. Tilgjengelig fra https://www.rand.org/pubs/research_reports/RR1577.html. [Lest 2017-05-09].

Raska, Michael (2015) *China and the 'Three Warfares'*. The Diplomat. [online], 2015-12-08. Tilgjengelig fra http://thediplomat.com/2015/12/hybrid-warfare-with-chinese-characteristics-2. [Lest 2017-08-16].

Rasmussen, Jens (1997) Risk management in a dynamic society: A modelling problem. *Safety Science* Vol. 27 No. 2/3 ss. 183-213.

Rasmussen, Mikkel Vedby (2001) Reflexive Security: NATO and International Risk Society. *Millennium* 30 (2) ss. 285-309.

Rathmell, Andrew (2002) Towards Postmodern Intelligence. *Intelligence and National Security* 17 (3 (Autumn 2002), ss.87-104.

Ravndal, Øyvin (2016) *Økt russisk operativ evne - Implikasjoner for Norges evne til å avverge eller motstå et væpnet angrep* [online], Masteroppgave. Oslo: Forsvarets høgskole. Tilgjengelig fra https://brage.bibsys.no/xmlui/handle/11250/2391885. [Lest 2017-10-13].

Reichborn-Kjennerud, Erik og Cullen, Patrick J. (2016) What is Hybrid Warfare? *NUPI Policy Brief* [online] 1, (2016) ss.1-4. Tilgjengelig fra https://brage.bibsys.no/xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf?sequence=3&isAllowed=y. [Lest 2017-08-05].

Renn, Ortwin (2006) *Risk Governance - Towards an Integrated Approach* [online], Geneva: International Risk Governance Council. Tilgjengelig fra http://https://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf. [Lest 2016-08-04].

Renz, Bettina og Smith, Hanna red. (2016) *Russia and Hybrid Warfare - Going Beyond the Label. Aleksanteri Papers 1/2016* [online] Helsinki: Aleksanteri Institute. Tilgjengelig fra https://helda.helsinki.fi/handle/10138/175291. [Lest 2017-08-05]

Rid, Thomas (2017) *Disinformation - A Primer in Russian Active Measures and Influence Campaigns (Hearings Before the Select Committee on Intelligence, US Senate)* [online], Washington D.C. Tilgjengelig fra https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf. [Lest 2017-07-30].

Rinelli, Sebastian og Duyvesteyn, Isabelle (2017) The Missing Link: Civil-Military Cooperation and Hybrid Wars. I: Cusumano, Eugenio og Corbe, Marian red. *A Civil-Military Response to Hybrid Threats*. Cham, Sveits: Palgrave Macmillan, ss. 17-39.

Røsland, Marit B. (2017) *Russland og ønsket om norsk alenegang* [online]. Tilgjengelig fra https://www.regjeringen.no/no/aktuelt/norsk_alenegang/id2544341/. [Lest 2017-11-16].

Olav Riste (2007) Intelligence and the 'Mindset': The German invasion of Norway in 1940. *Intelligence and National Security*, 22:4, ss. 521-536.

Rodnikovskij, Y. (1984) *Боевой устав воздушно-десантных войск. Часть II (батальон, рота)* [online] Moskva: Воениздат. Tilgjengelig fra http://militera.lib.ru/regulations/russr/1984_bu-vdv/index.html. [Lest 2017-08-17].

Rothkopf, David J. (2014) *National Insecurity – American leadership in an Age of Fear* [kindle]. Tilgjengelig fra www.amazon.com. [Lest 2017-11-11].

Saalman, Lora (2017) New domains of crossover and concern in cyberspace [online]. Stockholm: Stockholm International Peace Research Institute. Tilgjenglig fra: New Domains of Crossover and Concern in Cyberspace - SIPRI. [Lest 2017-11-09].

Sagan, Scott D. (1993) *The Limits of Safety: Organizations, Accidents and Nuclear Weapons*. Ss. 3-52. Princeton: Princeton University Press.

Saugumo Departamentas (VSD). Tilgjengelig fra https://kam.lt/download/53705/aotd%20gresmes%202016-en-el.pdf. [Lest 2017-08-20].

Schadlow, Nadia (2015) The Problem With Hybrid Warfare. *War on the Rocks*. [Blog] 2015-04-02. Tilgjengelig fra https://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/. [Lest 2017-08-05].

Schoitsch, Erwin (2005) *Design for safety and security of complex embedded systems: A unified approach* [online] Gdansk: NATO advanced research workshop on cyberspace security and defence. Tilgjengelig fra https://www.researchgate.net/profile/Erwin_Schoitsch/publication/251421683_Design_for_Safet

y_and_Security_of_Complex_Embedded_Systems_A_Unified_Approach/links/5774db1a08aeb9427e24a98f.pdf?origin=publication_list. [Lest 2017-08-07].

Shambaug, George (2002) Economic Warfare. in *Encyclopædia Britannica*. Vol. [online] :. Tilgjengelig fra https://www.britannica.com/topic/economic-warfare. [Lest 2017-08-11].

Singer, J. David (1958) Threat-perception and the armament-tension dilemma[online]. *Conflict Resolution* Volume II Number I ss. 90-105. Tilgjengelig fra http://journals.sagepub.com/doi/abs/10.1177/002200275800200110. [Lest 2017-11-15].

Snow, Nancy (2017) Public diplomacy in a national security context. I: Dunn Cavelty, Myriam og Balzacq, Thierry (2017) *Routledge Handbook of Security Studies* [kindle]. Tilgjengelig fra https://www.amazon.com. [Lest 2017-11-11].

Society for Risk Analysis (2015) *SRA glossary* [online] Tilgjengelig fra http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf. [Lest 2017-08-15].

Statsministeren (2012) *Rapport fra 22. juli-kommisjonen*. NOU 2012:14. Oslo: Statsministeren.

Statsministerens kontor/SMK (2017a) *Om r-konferanser* [online]. Tilgjengelig fra https://www.regjeringen.no/contentassets/b2dd39c6c22e4d32b508e0a4d82ba914/no/pdfs/b-0504-b_om-rkonferanser.pdf. [Lest 2017-11-14].

Statsministerens kontor/SMK (2017b) *Norway to join international centre for countering hybrid threats* [online]. Tilgjengelig fra https://www.regjeringen.no/en/aktuelt/norway-to-join-international-centre-for-countering-hybrid-threats/id2564689/. [Lest 2017-11-16].

Statsministerens kontor/SMK (2015) *Nytt sekretariat for Regjeringens Sikkerhetsutvalg (RSU)* [online]. Tilgjengelig fra https://www.regjeringen.no/no/aktuelt/nytt-sekretariat-for-regjeringens-sikkerhetsutvalg-rsu/id2427856/. [Lest 2017-11-15].

State Security Department of the republic of Lithuania (VSD) (2016) *National Security Threat Assessment* [online], Vilnius: State Security Department of the republic of lithuania/Valstybes

Statoil ASA (2013) *The In Amenas Attack* [online]. Tilgjengelig fra https://www.statoil.com/content/dam/statoil/documents/In%20Amenas%20report.pdf. [Lest 2017-11-13].

Statsrådets kansli (u.å.) Strategisk kommunikation [online]. Tilgjengelig fra http://vnk.fi/sv/strategisk-kommunikation. [Lest 2017-11-15].

Stoltenberg, Jens (2015) *Keynote speech: NATO Transformation Seminar* [online] Brussels: NATO. Tilgjengelig fra http://www.nato.int/cps/en/natohq/opinions_118435.htm. [Lest 2018-08-20].

Svechin, Aleksandr (1926) *Стратегия* [online], Moskva: Госвоениздат. Tilgjengelig fra http://http://militera.lib.ru/science/svechin1/index.html. [Lest 2017-08-17].

Thiele, Ralph (2016) Hybrid Threats – And how to counter them. *ISPSW Strategy Series: Focus on Defense and International Security* [online] No. 448, (Sep 2016) ss.1-12. Tilgjengelig fra http://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf. [Lest 2017-08-05].

Townsend, Mark (2017) Russia puts British Putin critic on Interpol wanted list. *The Guardian* [online] 2017-10-22. Tilgjengelig fra: https://www.theguardian.com/world/2017/oct/21/russia-british-businessman-bill-browder-interpol. [Lest 2017-10-23].

Tuck, Chris. (2017) Hybrid War: The Perfect Enemy. [Blog] *Defence-In-Depth*. Tilgjengelig fra https://defenceindepth.co/2017/04/25/hybrid-war-the-perfect-enemy. [Lest 2017-08-04].

Turner, Barry A., og Pidgeon, Nick F. (1997) *Man-made Disasters*. 2 edn. Oxford: Butterworth-Heinemann.

Turner, Barry A. (1976) 'The Organizational and Interorganizational Development of Disasters'. *Administrative Science Quarterly* 21 (3 (Sep. 1976), ss.378-397.

UNODA (2016) *Developments in the field of information and telecommunications in the context of international security* [online], Tilgjengelig fra https://www.un.org/disarmament/topics/informationsecurity/. [Lest 2017-08-05].

US Army SOC. (2015) *SOF Support to Political Warfare White Paper* [online] : United States Army Special Operations Command. Tilgjengelig fra https://dl.dropboxusercontent.com/u/6891151/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf. [Lest 2017-08-16].

US Department of State (2016). *Country Reports on Human Rights Practices for 2016* [online], US Department of State. Tilgjengelig fra https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper. [Lest 2017-10-17].

Utenriksdepartementet (2015) *Globale sikkerhetsutfordringer i utenrikspolitikken. Meld. St. 37.*. Oslo: Utenriksdepartementet.

Utenriksdepartementet/UD (2013) *Terrorangrepet på gassproduksjonsanlegget i In Amenas - Evaluering av norske myndigheters krisehåndtering*. Oslo: Utenriksdepartementet

USC Center on Public Diplomacy (u.å.) *Defining Public Diplomacy* [online]. Tilgjengelig fra https://uscpublicdiplomacy.org/page/what-pd. [Lest 2017-10-01].

Vandepeer, Charles (2011) *Rethinking Threat: Intelligence, Analysis, Intentions, Capabilities and the Challenge from Non-state Actors* [online]. Phd. Thesis, The University of Adelaide. Tilgjengelig fra

https://digital.library.adelaide.edu.au/dspace/bitstream/2440/70732/8/02whole.pdf. [Lest 2017-11-13].

Van Messel, John A. (2005) *Unrestricted Warfare: A Chinese doctrine for future warfare?* [online], Master of Operational Studies Dissertation. Quantico: United States Marine Corps School of Advanced Warfighting. Tilgjengelig fra http://www.dtic.mil/dtic/tr/fulltext/u2/a509132.pdf. [Lest 2017-08-16].

Voyger, Mark. (2015) Russia's Use of the Legal Element of Hybrid Warfare. *Land Power Magazine* [online], Spring 2015, Vol. 1, Issue 2. Tilgjengelig fra https://www.lc.nato.int/resources/site1/general/media_center/landpowervolume1issue2_web4.pdf. [Lest 2017-10-17].

Westrum, Ron og Adamski, Anthony J. (2009) Organizational Factors Associated with Safety and Mission Success in Aviation Environments. I: Wise, John A., Hopkin, V. David og Garland, Daniel J. red. (2009) *Handbook of Aviation: Human Factors*. 2nd edition. Boca Raton: CRC Press.

Widerberg, Charlotte H. (2017) *Why do Two Liberal Democracies have Significantly Diverging Legal Powers to Access Digital Communications for Countering the Same range of Threats, and what are the Implications for their Security?* Master's thesis. King's College London.

Wohlstetter, Roberta (1962) *Pearl Harbor – Warning and Decision*. Stanford: Stanford University Press.

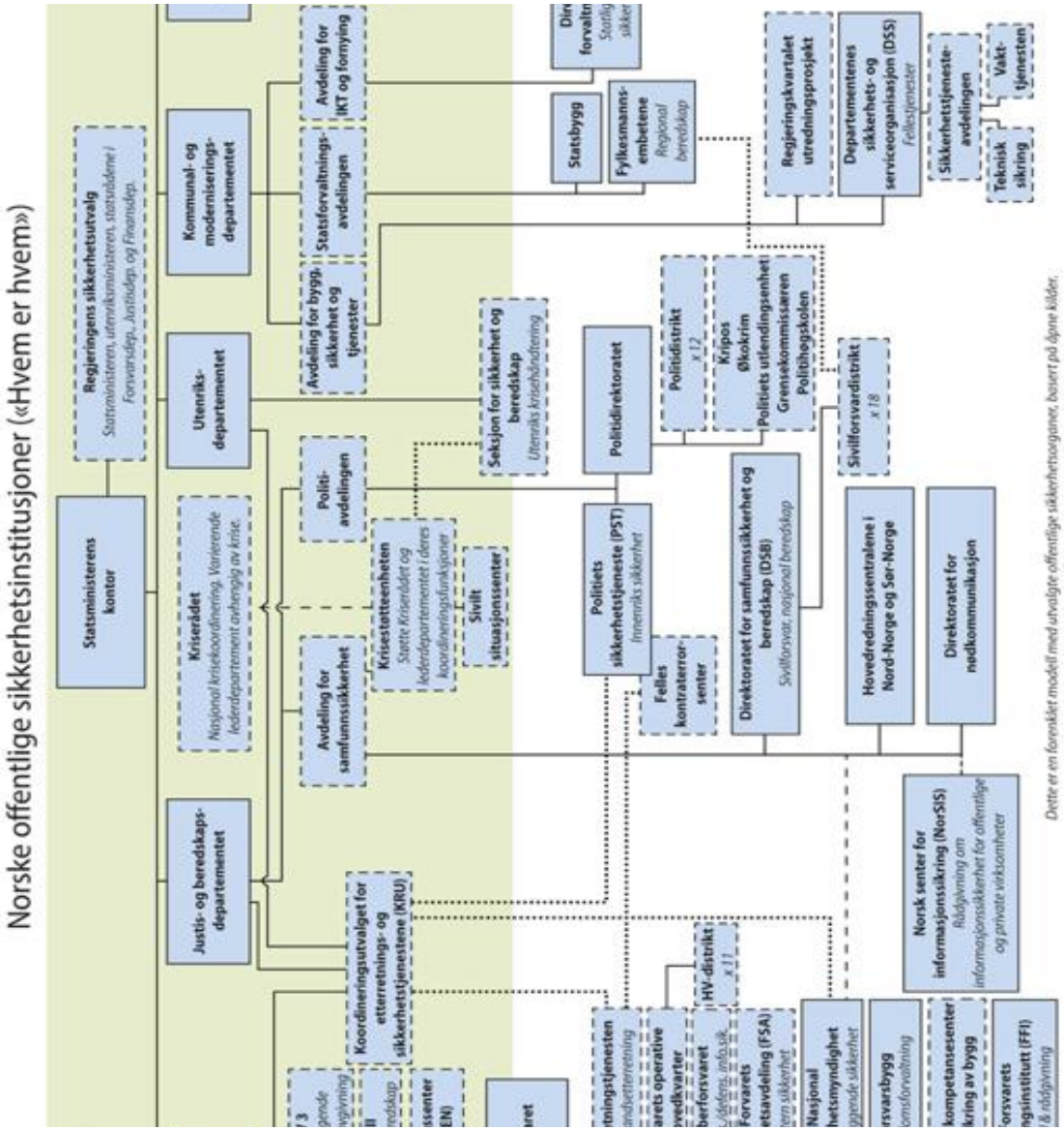
Wolfers, Arnold. (1962) *Discord And Collaboration: Essays On International Politics* [online], Baltimore: The Johns Hopkins Press. Tilgjengelig fra http://https://ia600500.us.archive.org/33/items/discordandcollab012923mbp/discordandcollab012923mbp.pdf. [Lest 2017-08-08].

Zatulin, Konstantin F. (2016) *Гражданство РФ для «носителей русского языка». Проект № 69201-7 внесен 30.12.2016 депутатом Государственной Думы К.Ф. Затулиным* [online], Tilgjengelig fra https://zatulin.ru/grazhdanstvo-rf-dlya-nositelej-russkogo-yazyka.html. [Lest 2017-10-17].

Öhme, Richard. (2017) *Psykologiskt försvar - Informationspåverkan och cyberförmåga* [presentasjon]. Tilgjengelig fra https://www.nsm.stat.no/globalassets/dokumenter/sikkerhetskonferansen-2017/presentasjoner/msb-cyber--informationspaverkan-2017-03-29.pdf. [Lest 2017-06-03].

8. Vedlegg

Vedlegg A: Norske offentlige sikkerhetsinsitusjoner



Kilde: NOU 2016: 19 *Samhandling for sikkerhet* (JBD 2016c)

Vedlegg B: Hybridbegrepets historie og innhold

Hybridbegrepet ble først benyttet i amerikanske militære kilder med referanse til ikke-statlige aktører som tok i bruk en kombinasjon av konvensjonelle og ikke-konvensjonelle militære virkemidler i tillegg til ikke-militære virkemidler (Hoffman 2014). General James Mattis, den gang sjef for US CENTCOM og US Marines-offiseren Frank Hoffman beskrev i 2005 en fremvekst av "irregulære metoder" som terrorisme, opprørstaktikk og narkotikakriminalitet. "Irregulære utfordrere forsøker å utnytte taktiske fordeler på steder og tidspunkter de selv velger, i stedet for å spille etter våre regler. De forsøker å akkumulere en rekke mindre taktiske effekter, forstørre disse gjennom media og gjennom informasjonskrigføring for å svekke USAs kampvilje. [...] Denne hittil ukjente syntesen kaller vi hybrid krig" (Mattis og Hoffman 2005).

Hizbollah i konflikten mellom Israel og Libanon i 2006 er et hyppig brukt eksempel på en ikke-statlig aktør som har tatt i bruk virkemidler som tradisjonelt tilhører stater. Gruppen benyttet blant annet avanserte missiler, UAV og cyber-angrep, samtidig som de iverksatte en sofistikert mediekampanje for å vinne "hearts and minds" (Karlsen 2010).

ISIL har tilsynelatende utviklet Hizbollah-modellen videre. De er til dels et terrornettverk, dels en geriljahær og dels en proto-stat. Gruppen benytter både konvensjonelle og irregulære taktikker og et bredt våpenarsenal på slagmarken. Som terrornettverk gjennomfører (eller inspirerer de til) angrep mot myke mål i vestlige land, de støtter seg på sosiale medier for å fremme sin sak og for å rekruttere nye medlemmer. De finansieres delvis gjennom donasjoner, delvis gjennom salg av olje, hvete og antikviteter og delvis gjennom løsepenger og midler fra utpressing (Thiele 2016:3).

Den teknologiske og sosio-økonomiske utviklingen har gradvis visket ut skillet mellom metoder som statlige og ikke-statlige aktører benytter i krigføring. Moderne teknologi har økt dødeligheten, effektiviteten og rekkevidden til ikke-statlige aktører som Hizbollah og ISIL. Samtidig har Russland vist at stater kan utnytte motstanderens sårbarheter i den lavere enden av konfliktspekteret gjennom å bruke informasjonsoperasjoner og irregulære taktikker. Ikke-statlige aktører griper med andre ord etter virkemidler som ligger høyere i konfliktspekteret, mens stater søker seg nedover i spekteret (Sari 2017:6, Giegerich 2015:13).

Ofte blir den russiske generalstabssjefen V. Gerasimovs artikkel "Vitenskapens prediktive verdi/Ценность науки в предвидении" trukket frem som en "oppskrift" på hvordan Russland tenker rundt hybridkrig. I artikkelen peker Gerasimov på at "en velfungerende stat i løpet av måneder eller dager kan forvandles til en arena med harde væpnede kamper, bli offer for utenlandske intervensjoner og synke ned i en avgrunn av kaos, humanitær katastrofe og borgerkrig" (Gerasimov 2013). Gerasimov beskriver et 1:4-forhold mellom militære og ikke-militære maktmidler i moderne konflikter, der de ikke-militære inkluderer politisk/diplomatisk press, økonomiske sanksjoner, etablering av politisk opposisjon og informasjonsoperasjoner, som utføres både i det militære og ikke-militære domenet (*ibid.*). Gerasimov benytter imidlertid ikke betegnelsen ”hybridkrig” i sin artikkel. Det gjør han derimot i artikkelen ”Fred på grensen til krig/Мир на гранях войны” (Gerasimov 2017), der han beskriver hvordan USA og NATO i økende grad benytter en kombinasjon av militære og ikke-militære midler i internasjonale konflikter.

Enkelte kommentatorer påpeker at artikkelen kun er en reaksjon fra russisk hold på antatt vestlig innblanding i interne politiske prosesser i andre land, og et forsøk på å beskrive miljøet russiske væpnede styrker i dag må forventes å kunne operere i (Bartles 2016, Kofman 2016). Mark Galeotti peker imidlertid på at det å bruke andre lands strategier som en allegori for å omtale sine egne strategier er en russisk tradisjon som strekker seg tilbake til Sovjet-tiden (Manea 2015).

Også i russiskspråklige kilder finner man referanser til konsepter som viser at det som i dag omtales som hybride trusler langt fra er noe som har oppstått i løpet av de siste årtiene.

Aleksandr Svechin beskrev på 1920-tallet konseptet ”utmattelseskrig” (измор) som innbefatter å benytte politiske og økonomiske virkemidler for å undergrave en annen stat uten at militære maktmidler kommer til anvendelse. Metodevalget må være tilpasset situasjonen. Svechin viser til Lenin, som hadde et klart bilde av det endelige målet, men en pragmatisk og fleksibel måte for å komme dit (Svechin 1926).

Den antikommunistiske russiske eksil-offiseren og militærteoretikeren Evgeniy Messner har blitt kalt ”hybridkrigens bestefar” (Klus 2016). Hans skrifter ble i 2005 samlet og utgitt av i en militær monografiserie med tittelen *Ønsker du fred, må du vinne opprørskrigen/Хочешь мира, победи мятежевойну* (Messner 2005). Her beskriver han hvordan moderne konflikter utkjempes i gråsonen mellom krig og fred, der de stridende benytter seg av en blanding av konvensjonelle og ikke-konvensjonelle midler, der frontlinjene er uklare, og der det psykologiske domenet står sentralt (Klus 2016, Myasnikov 2005). Messner skrev på 1960-tallet, med atomkappløpet og stedfortrederkriger i Afrika og Asia som bakteppe. Han forklarer fremveksten av ”opprørskrigen” med at eksistensen av atomvåpen hadde gjort en krig mellom USA og Sovjetunionen ekstremt farlig, og at de to statene hadde sett seg nødt til å ”i stedet for å splitte hydrogenatomer, heller splitte fiendebefolkningens atomer, det vil si deres ånd, deres psyke” (Messner 2005:129). Messner slår fast at ”i psykologisk krigføring er ikke seier i et slag eller territorielle fremganger et mål i seg selv: de er verdifulle først og fremst gjennom sin psykologiske effekt. For Israel ville det vært psykologisk tyngre å miste det mystiske Jerusalem enn å miste hovedstaden og havnebyen Tel Aviv” (*ibid.* 2005:130). Messner peker også på betydningen av agitasjon, det vi i dag ville kalt ”strategisk kommunikasjon”: ”Agitasjon i krig må være tosidig – en halvsannhet for våre egne, en annen halvsannhet for fienden” (*ibid.*: 134).

En sammenligning av to historiske og to nyere eksempler der stater har valgt hybride virkemidler for å oppnå politiske mål (forsøket på en kommunistisk revolusjon i Tyskland i 1923, Nazi-Tysklands anneksjon (Anschluss) av Østerrike i 1936, Georgia-krigen i 2008 og anneksjon av Krym fulgt av konflikten i Donbass i 2014) viser at faktorer som grad av støtte i lokalbefolkningen, maktforholdet mellom angriper og forsvarer og konfliktens lengde er sentrale for om et hybrid angrep lykkes eller ikke (Neville 2015).

Vedlegg C: Konsistensmatrise

Konsistensmatrisen viser alle parameterverdiene i analysen. X indikerer at et par er vurdert som inkonsistent (spesialstyrker er ikke del av økonomiske tiltak). Mulige kombinasjoner er markert med et åpent felt. Gjennom å vurdere hvilke verdipar som er mulige og hvilke som er umulige kan vi kartlegge mulige løsninger på problemet. Konsistensmatrisen bidrar også visuelt til kravet om at analysen skal være åpen og etterprøvbar.

	militært	politisk	informasjon	økonomisk	fordekt	kjernefysiske styrker	spesialstyrker	konvensjonelle styrker	organisert kriminalitet	stedfortredergrupper	etterretningstjeneste	diplomati	redigerte medier	sosiale medier	NGO	næringsliv	rettsvesen	hackergrupper	offensiv mil operasjon	militært press	multilateralt diplomati	bilateralt (tvangs)diplomati	støtte stedfortredergrupper	etablere de facto tilstedeværelse	public diplomacy	propagandaoperasjon	sanksjoner	implisert økonomisk tvang	manipulere internasjonal rett	utforming av lover	rettsforfølge nasjonalt	fordekte operasjoner	vold v/stedfortreder	cyberangrep
militært																																	
politisk																																	
informasjon																																	
økonomisk																																	
sivilt																																	
fordekt																																	
kjernefysiske styrker		X	X	X	X																												
spesialstyrker		X	X	X																													
konvensjonelle styrker		X	X	X	X																												
organisert kriminalitet	X	X	X	X																													
stedfortredergrupper	X	X	X	X																													
etterretningstjeneste	X	X	X	X																													
diplomati	X		X	X	X																												
redigerte medier	X	X		X	X																												
sosiale medier	X	X		X	X																												
NGO	X		X	X	X																												
næringsliv	X		X		X																												
rettsvesen	X		X		X																												
hackergrupper	X	X	X	X																													
offensiv mil operasjon		X	X	X	X	X			X	X	X	X	X	X	X	X	X	X															
militært press		X	X	X	X				X	X	X	X	X	X	X	X	X	X															
multilateralt diplomati	X		X	X	X	X	X	X	X	X	X		X	X	X	X	X	X															
bilateralt (tvangs)diplomati	X		X	X	X	X	X	X	X	X	X		X	X	X	X	X	X															
støtte stedfortredergrupper	X		X	X	X	X	X	X	X	X			X	X			X	X															
etablere de facto tilstedeværelse	X		X	X	X	X	X	X	X	X	X	X	X	X			X	X															
public diplomacy	X		X	X	X	X	X	X	X						X	X	X	X															
propagandaoperasjon	X	X		X	X	X	X	X	X			X			X	X	X	X															
sanksjoner	X	X	X		X	X	X	X	X	X	X		X	X	X	X	X	X															
implisert økonomisk tvang	X	X	X		X	X	X	X		X		X	X	X	X		X	X															
manipulere internasjonal rett	X		X	X	X	X	X	X	X	X	X		X	X	X	X		X															
utforming av lover	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X		X															
rettsforfølge nasjonalt	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X		X															
fordekte operasjoner	X	X	X	X		X		X		X		X	X	X	X	X	X	X															
vold v/stedfortreder	X	X	X	X		X	X	X				X	X	X	X	X	X	X															
cyberangrep		X	X	X		X	X			X		X	X	X	X	X	X																