FFI-RAPPORT

21/00246

Situasjonsforståelse ved sammensatte trusler

— et konseptgrunnlag

Stein Malerud
Alf Christian Hennum
Narve Toverød

Situasjonsforståelse ved sammensatte trusler – et konseptgrunnlag

Stein Malerud
Alf Christian Hennum
Narve Toverød

Forsvarets forskningsinstitutt (FFI) 2. februar 2021

Emneord
Hybridkrigføring
Situasjonsforståelse
Trusler
Totalforsvar

FFI-rapport
21/00246

Prosjektnummer
1499

Elektronisk ISBN
978-82-464-3326-4

Engelsk tittel
Situation awareness encountering hybrid threats – a conceptual basis.

Godkjennere
Alf Christian Hennum, *forskningsleder*
Sigurd Glærum, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

God situasjonsforståelse er en forutsetning for å kunne ta gode og tidsriktige beslutninger, men den utfordres i møte med sammensatte trusler. Hensikten med denne rapporten er å støtte utviklingen av et konsept for å bedre nasjonal situasjonsforståelse i møte med sammensatte trusler.

Konseptgrunnlaget er utarbeidet av FFI-prosjektet Multinational Capability Development Campaign (MCDC) som en del av FFIs forskning på hybrid krigføring og sammensatte trusler. Prosjektets hovedformål er å tilgjengeliggjøre kunnskap fra MCDC-aktivitetene *Countering Hybrid Warfare* (CHW) I-III i et nasjonalt perspektiv. Innholdet i rapporten er derfor basert på funn og anbefalinger fra MCDC CHW, sammen med innspill fra flere nasjonale og internasjonale workshoper rundt temaet sammensatte trusler. Informasjon fra disse er videre sett i lys av styrende dokumenter og relevant faglitteratur.

Vi bruker begrepsforståelsen fra MCDC CHW: Sammensatte (hybride) trusler er «synkronisert bruk av ulike maktmidler for å ramme spesifikke sårbarheter i hele bredden av samfunnsfunksjoner for å oppnå synergistiske effekter». Maktmidlene kan være av både militær, politisk, økonomisk, sivil, informasjonsmessig og juridisk art og benyttes mot sårbarheter innenfor alle samfunnssektorene.

Sammensatte trusler kan opptre i hele krisespektret fra fred til full konflikt. I denne rapporten ser vi spesielt på gråsonen mellom fred og krise hvor skillet mellom samfunnssikkerhet og statssikkerhet er mer utydelig. Her vil en aktør kunne utnytte egenskaper ved sammensatte trusler for å nå egne målsettinger samtidig som han utfordrer vår evne til å oppnå situasjonsforståelse. I rapporten kommer vi med forslag og anbefalinger om hvordan man kan bedre evnen til situasjonsforståelse i møte med sammensatte trusler.

Situasjonsforståelse er en individuell egenskap som avhenger av mange faktorer. Grunnleggende er tilgjengelighet på relevant informasjon om trusler, sårbarheter og viktige samfunnsfunksjoner. Sammensatte trusler krever at man deler informasjon om trusler og effekter på tvers av sektorer. Videre kreves det at man evner å se enkelthendelser innenfor ulike sektorer i sammenheng og forstå den akkumulerte effekten på samfunns- og statssikkerheten sett i lys av mulige trusselaktørers mål og intensjoner.

I rapporten anbefaler vi blant annet at det etableres et tverrsektorielt situasjonsbilde for å støtte tverrsektoriell situasjonsforståelse. Situasjonsbildet inngår i beslutningsgrunnlaget som skal svare på beslutningstakeres informasjonsbehov rundt forebygging og håndtering av denne type trusler. Videre anbefaler vi å etablere en strategisk analysekapasitet for å bygge og vedlikeholde situasjonsbilde og beslutningsgrunnlag.

Summary

Situation awareness is a premise for making sound and timely decisions. However, hybrid threats challenge the ability to obtain situation awareness. The purpose of this report is to support the future development of a concept aiming to improve the national situation awareness in encountering hybrid threats.

This report is written by the FFI project Multinational Capability Development Campaign (MCDC) as a part FFI's research on hybrid threats. One important objective of the project is to make available results from the MCDC activities Countering Hybrid Warfare (CHW) I-III in a national context. Hence, the content of the report is based on results and recommendations from the MCDC CHW activities together with input from several national and international workshops.

In the report, we use the MCDC CHW definition of the term hybrid threats: «*the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*». The instruments of power covers military, political, economical, civil, information and legal means, combined to exploit vulnerabilities within various societal sectors.

Hybrid threats appear in every part of the conflict spectrum, from peace to military conflict and war. In this report, we focus on the « grey zone» in between peace and conflict where the border between societal security and state security is blurred. In the grey zone, a threat actor can exploit properties of hybrid threats in order to achieve short and long-term objectives simultaneously challenging our situation awareness. This report provides suggestions and recommendations on how we can improve the ability to obtain situation awareness facing hybrid threats.

The ability to obtain situation awareness is individual and depends on several factors. However, fundamental is the availability of information about threats, vulnerabilities, effects and the state of the societal functions. The nature of hybrid threats requires mechanisms for sharing information about threats and effects between different sectors across society. Further, it is necessary to understand the accumulated effect of single incidents on the societal and state security, and whether the effects are in line with anticipated goals and objectives of potential adversaries.

In this report, we recommend the establishment of a cross-sectorial situation picture to support cross-sectorial situation awareness. The situation picture is a part of the decision basis developed to support decision making with respect to preventing and managing hybrid threats. Further, we recommended establishing a strategic capacity for the analysis of hybrid threats.

Innhold

Forord

Denne rapporten er skrevet som en del av FFI-prosjektet 1499 MCDC på oppdrag fra Forsvarsdepartementet. Et sentralt mål for rapporten har vært å tilgjengeliggjøre kunnskap og anbefalinger fra MCDC-aktivitetene *Countering Hybrid Warfare* (CHW) I-III i et nasjonalt perspektiv.

Det ble etablert en referansegruppe for prosjektet med eksperter fra ulike organisasjoner som har ansvar for eller har interesse av å bidra til nasjonal krisehåndtering. Det ble arrangert én workshop med denne gruppen. Det var planlagt en workshop til, men denne ble avlyst på grunn av Covid-19. Vi fikk i stedet mulighet til å bidra i en workshop arrangert i regi av langtids-planarbeidet i politiet. Denne ble gjennomført høsten 2020, og dreide seg om hvordan sammensatte trusler kan ramme samfunnet og utfordringene med å etablere tilstrekkelig situasjonsforståelse. I tillegg er det arrangert to workshop'er i regi av det britiske, nederlandske og norske forskningssamarbeidet ANNCP[1] med tema sammensatte trusler og situasjonsforståelse.

Vi ønsker å takke alle som har bidratt med informasjon og kommentarer til arbeidet med denne rapporten.

Kjeller, 2. februar 202

Stein Malerud, Alf Christian Hennum og Narve Toverød

[1] Anglo, Netherlands, Norwegian collaboration projects.

1 Innledning

1.1 Bakgrunn og hensikt

Denne rapporten er utarbeidet i FFI-prosjekt 1499 Multinational Capability Development Campaign (MCDC) som en del av FFIs forskning på hybrid krigføring og sammensatte trusler. FFI-prosjektets hovedformål er å tilgjengeliggjøre kunnskap fra MCDC-aktiviteten Countering Hybrid Warfare (CHW) I-III i et nasjonalt perspektiv.

Multinational Capability Development Campaign (MCDC) er et USA-ledet initiativ som ble etablert i 2003 som Multinational Experiment (MNE). MCDC er et internasjonalt samarbeid som adresserer multinasjonale kapabilitets-utfordringer. Arbeidet er organisert i kampanjer hvor interesserte nasjoner/ institusjoner kan foreslå tema og melde seg på. Kampanjene har to års varighet og man kan være aktiv bidragsyter eller observatør. Hver kampanje skal resultere i et sluttprodukt.

MCDC-samarbeidet har gjennomført to prosjekter innenfor temaet *Countering Hybrid Warfare* (CHW). Det første, CHW I (2015–2016), dreide seg om å øke forståelsen for hybrid krigføring/påvirking. Det andre, CHW II (2017–2018), så på hvordan man kan øke evnen til å motvirke hybride trusler. MCDC er nå i ferd med å avslutte det tredje prosjektet, CHW III (2019–2020). Dette har som mål å utarbeide en håndbok som beskriver hvordan man kan benytte operativ planlegging for å forebygge og håndtere sammensatte/hybride trusler.

Hensikten med rapporten er å bidra til arbeidet med å forbedre situasjonsforståelsen i møte med sammensatte/hybride trusler. Rapporten er skrevet som et konseptgrunnlag. I dette ligger det at rapporten skisserer et grunnlag for utviklingen av et fremtidig konsept[2] for å bedre situasjons-forståelsen rundt sammensatte/hybride trusler. Konseptgrunnlaget bidrar med forslag, ideer og tiltak for hvordan situasjonsforståelse kan oppnås ved å ta utgangspunkt i utfordringene sammensatte trusler gir for evnen til å oppnå god situasjonsforståelse.

MCDC CHW-prosjektene tar for seg både det å oppdage, avskrekke og håndtere sammensatte trusler. Vi har i denne rapporten valgt å gå mer i dybden rundt problemet med å oppdage og forstå at man er utsatt for sammensatte trusler, det vil si evne til å oppnå situasjonsforståelse. God situasjonsforståelse er en forutsetning for å kunne ta gode og tidsriktige beslutninger i forbindelse med forebygging og håndtering av uønskede hendelser i fred, krise og krig. Sammensatte trusler utfordrer evnen til å oppnå situasjonsforståelse ved at de kan skape

[2] Store norske leksikon (www.snl.no): Konsept betyr samling av ideer eller en plan som danner grunnlaget for utformingen av et produkt, arrangement eller en virksomhet.

usikkerhet og forvirring rundt om man faktisk er utsatt for en kampanje, og hva som eventuelt er aggressors mål og intensjoner.

I henhold til begrepsbruken i MCDC CHW kan sammensatte/hybride trusler forstås som «*synkronisert bruk av ulike maktmidler for å ramme spesifikke sårbarheter i hele bredden av samfunnsfunksjoner for å oppnå synergistiske effekter*»[3]. I dette ligger det å sette sammen ulike metoder og virkemidler, både lovlige og ulovlige, til en pakke/kampanje som kan ramme sårbarheter i alle deler av samfunnet i fredstid, under sikkerhetspolitiske kriser og i konflikt/ krig. Den samlede effekten vil kunne true norsk suverenitet og handlefrihet. Spesielt utfordrende er sammensatte trusler som opererer i gråsonen[4] mellom fred og krise/konflikt og som kan true både samfunns- og statssikkerheten. Samfunnssikkerhet er i henhold til Store norske leksikon (snl.no) evnen samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påvirkninger. Statssikkerhet innebærer å ivareta sikkerhetsbehov relatert til statens eksistens, suverenitet og integritet (FD/JD, 2018, s.12)

Sammensatte trusler og gråsoneproblematikk vies stadig større oppmerksomhet innenfor arbeidet med samfunns- og statssikkerheten. Dette er viktige tema i blant annet i Prop. 14 S – langtidsplan for forsvarssektoren. (FD, 2020) og Meld. St. 5 – samfunnssikkerhetsmeldingen (JD, 2020). Begge disse dokumentene poengterer at det er en økende grad av sammenheng mellom samfunns- og statssikkerhet. Bortfall av eller utilgjengelige kritiske samfunnsfunksjoner (DSB, 2017) utfordrer samfunnssikkerheten direkte, men kan også ha konsekvenser for statssikkerheten.[5] Sammensatte trusler er derfor en tverrsektoriell utfordring som spenner over alle nivåer innen både statsforvaltningen og lokal forvaltning. I Prop. 14 S (2020–2021) poengteres det: «*Gråsone-situasjoner utfordrer vår forståelse av stats- og samfunnssikkerhet som to klart adskilte begreper*» (FD, 2020, s. 73).

Forsvarets viktigste oppgaver er knyttet til å ivareta statssikkerheten under kriser og krig/ konflikt i samarbeid med andre totalforsvarsaktører og allierte. Sammensatte trusler / hybrid krigføring er ikke et nytt fenomen i krig og konflikt. Ofte kombineres regulære militære maktmidler med irregulære maktmidler for å forsterke effekten av de militære operasjonene. Denne rapporten ser først og fremst på hendelser i gråsonen hvor innslaget av irregulære maktmidler er større enn bruken av regulære (Diesen, 2018), men hvor uønskede hendelser og pakker med sammensatte trusler også kan påvirke statssikkerheten og Forsvarets daglige virksomhet og operative evne. Krisehåndtering i gråsonen er i utgangspunktet tillagt de ulike samfunnssektorene, kommunene og regionene i henhold til sektorprinsippet og krisehåndteringsprinsippene (JD, 2020).

[3] Cullen & Reichborn-Kjennerud (2017): «*the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*».

[4] From RAND report (RAND 2019) "…gray zone tactics as *ambiguous* political, economic, informational, or military actions that primarily target domestic or international public opinion and are employed to advance a *revisionist* nation's interests without provoking outright war.".

[5] Ivareta statens eksistens, suverenitet og integritet og politisk handlefrihet.

Rapporten er primært skrevet for personer som arbeider med å utvikle situasjonsforståelse hos norske myndigheter, men den kan også være av interesse for alle som arbeider med sammensatte trusler.

1.2 Fremgangsmåte og sentrale kilder

Arbeidet med dette konseptgrunnlaget har tatt utgangspunktet i funn og anbefalinger fra MCDC CHW-prosjektene:

- *Understanding hybrid warfare* (Cullen & Reichborn-Kjennerud, 2017)
- *Countering hybrid warfare* (Monaghan mfl., 2019)

I tillegg benyttes dokumentet *A description of two national conceptual approaches for establishing Hybrid threat/ Hybrid influence situation awareness* (Ferm mfl., 2018) som ble skrevet som et innspill til arbeidet i MCDC CHW II. Dokumentet beskriver og sammenlikner den finske og norske tilnærmingen til sammensatte trusler og situasjonsforståelse rundt disse.

I november 2019 ble det arrangert en workshop for å få innspill til arbeidet med et konseptgrunnlag. Her deltok ulike aktører med roller og ansvar innenfor samfunns- og statssikkerhet. På workshopen ble det benyttet en alternativ-analyseteknikk (*Starbursting*) (Nato, 2017) for å generere ideer rundt problemstillingen «*Hvilken informasjon forventer du å finne i et konsept til støtte for nasjonal situasjonsforståelse knyttet opp mot hybride trusler?*». Dette ga mange innspill som er dokumentert i (Toverød mfl., 2020). Innspillene ble videre analysert og gruppert i tema som danner grunnlaget for innholdet i konseptgrunnlaget. Det ble også identifisert et behov for et nasjonalt konsept som beskriver hvordan man kan etablere og vedlikeholde situasjonsforståelse ovenfor sammensatte trusler som kan ramme Forsvaret og samfunnet for øvrig.

I oktober 2020 ble det arrangert en workshop til rundt temaet sammensatte trusler og situasjonsforståelse. Denne workshopen var todelt og et samarbeid mellom Justis- og beredskapsdepartementet (JD)/politiavdelingen og FFI. På første dag ble det gitt presentasjoner fra ulike aktører om relevante tema innen det å oppdage, attribuere og håndtere sammensatte trusler. På dag to ble det gjennomført en scenariodiskusjon med utgangspunkt i et scenario hvor en trusselaktør tar i bruk et bredt spekter av metoder og virkemidler for å ramme sårbarheter med effekter på tvers av samfunnssektorene. Resultatene herfra ga innblikk i informasjonsflyt, roller, ansvar og myndighet med hensyn til å oppdage og håndtere enkelttrusler, og videre problemstillinger rundt det å avdekke at enkelthendelsene er en del av en større kampanje med bruk av sammensatte trusler.

Det har vært gjennomført to workshoper i regi av Anglo, Netherlands and Norwegian Collaboration Projects (ANNCP) ved TNO i den Haag i mars 2019 og februar 2020.[6] Tema for disse workshopene var «*Assessment of hybrid conflicts/operations*». Under workshopene ble det lagt spesiell vekt på hvordan man kan understøtte situasjonsforståelse og etablere et godt beslutningsgrunnlag for forebygging og håndtering av sammensatte trusler.

Det sentrale temaet i dette grunnlaget er hvordan vi kan styrke situasjonsforståelsen i møte med sammensatte trusler. For å få en bedre forståelse av hva situasjonsforståelse er, benytter vi Endsleys modell (Endsley, 1995). Modellen beskriver tre nivåer av situasjonsforståelse og faktorer som påvirker disse. Denne er mer utførlig beskrevet i kapittel 2.2. Endsleys modell, sammen med typiske egenskaper ved sammensatte trusler, gir grunnlag for å identifisere en del utfordringer rundt det å oppnå situasjonsforståelse i møte med sammensatte trusler. I rapporten diskuteres disse utfordringene i lys av funnene fra MCDC CHW, workshopene og relevante dokumenter og litteratur.

1.3 Organisering av dokument

Konseptgrunnlaget er organisert i seks hovedkapitler:

- Kapittel 2 gir en beskrivelse av utfordringer ved sammensatte trusler og situasjonsforståelse.
- Kapittel 3 omhandler forutsetninger og rammer for utviklingen av et konsept.
- Kapittel 4 diskuterer konseptuelle løsninger rundt det å etablere et relevant situasjonsbilde og beslutningsgrunnlag ved sammensatte trusler.
- Kapittel 5 omhandler kunnskaps- og kompetansebehov.
- Kapittel 6 ser på teknologi og infrastruktur som kan understøtte situasjonsforståelse.
- Kapittel 7 avslutter rapporten og kommer med forslag og anbefalinger.

[6] Resultatene fra workshopene er dokumentert i to powerpoint-presentasjoner.

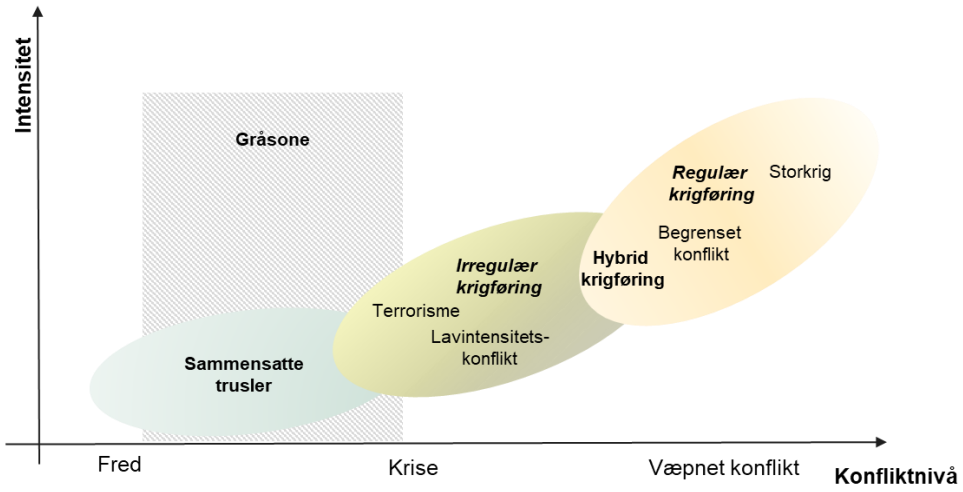
2 Sammensatte trusler og situasjonsforståelse

2.1 Sammensatte/hybride trusler

2.1.1 Hva er sammensatte/hybride trusler?

I henhold til begrepsforståelsen fra MCDC CHW I-III, som gjengitt i kapittel 1, innebærer bruk av sammensatte trusler at en angriper setter sammen ulike maktmidler som forsterker hverandre (MPECI) [7] i en angrepspakke eller til en kampanje rettet mot ulike sårbarheter hos motstanderen i PMESII-domenene[8] hvor den samlede/akkumulerte effekten understøtter motstanderens overordnede mål. DIMEFIL er et annet akronym som benyttes som oversikt over mulige maktmidler som kan benyttes i et angrep ved bruk av sammensatte trusler.[9]

Begreper som hybrid krigføring, hybride trusler, hybrid påvirkning og sammensatte trusler benyttes om hverandre. I dette konseptgrunnlaget er det fornuftig å benytte ett enhetlig begrep. Begrepet sammensatte trusler blir stadig vanligere og benyttes blant annet i Prop. 14 S (2020–2021) og Meld. St. 5 (2020–2021). Sammensatt er en norsk oversettelse av begrepet hybrid.[10]



Figur 2.1 Sammensatte trusler og hybrid krig. Basert på Monaghan, S., PRISM 8, no 2.

Sammensatte/hybride trusler kan opptre i hele konfliktspektret. Vi har her valgt å se spesielt på situasjoner i gråsonen mellom fred (daglig virksomhet) og krise/konflikt (se figur 2.1). Her vil trusselen typisk påvirke samfunnssikkerheten direkte, for eksempel ved angrep på samfunnskritiske funksjoner og infrastruktur. Men enkelte hendelser eller den samlede/akkumulerte

[7] MPECI: Military, Political, Economic, Civil, Information.
[8] PMESII: Political, Military, Economic, Social, Information, Infrastructure.
[9] DIMEFILmaktmidler: Diplomatic, Informational, Military, Economic, Finance, Intelligence and Law Enforcement (Legal). Se for eksempel: Aday (2019) eller https://www.whs.mil/News/News-Display/Article/2133177/putting-the-fil-into-dime-growing-joint-understanding-of-the-instruments-of-pow/
[10] Hybrid (norsk ordbok): noe som er sammensatt av ulike elementer.

effekten av flere hendelser vil også kunne utfordre statssikkerheten.[11] I denne gråsonen er det ikke noen etablert konflikttilstand, slik at det er naturlig å anta at lavintensitetstrusler dominerer i forhold til regulære militære trusler (Diesen, 2018). Krigføring er et begrep som assosieres med konflikt og krig hvor Forsvaret er hovedaktør. Derfor er det mer hensiktsmessig å benytte begrepet trusler enn krigføring i gråsonen.

2.1.2 Trussel

En trussel kan ses på som en kombinasjon av mål, metode (fremgangsmåte) og virkemiddel satt sammen for å ramme et angrepsmål. En sammensatt trussel kombinerer ulike trusler i en angrepspakke/kampanje for å nå mer overordnede strategiske mål. En slik kampanje kan være godt planlagt eller opportunistisk. En opportunistisk tilnærming innebærer at aktøren i større grad utnytter muligheter som dukker opp.

En forutsetning for at vi skal rammes av sammensatte trusler er at det finnes en aktør med et ønske (mål og intensjon) om å ramme oss, og som har de rette kapabilitetene til å gjøre det. I dette grunnlaget tenker vi først og fremst på stater som trusselaktører. Disse har evne og vilje til å bruke sammensatte trusler til å oppnå langsiktige strategiske mål. Eksempler på slike mål kan være strategisk posisjonering (øke egen innflytelse) og sikre egen suverenitet og handlefrihet. En stat vil kunne utnytte flere typer maktmidler innen MPECI/DIMEFIL til å påvirke oss i et kortsiktig og langsiktig tidsperspektiv. Selv om målet med bruk av sammensatte trusler som oftest er å oppnå strategiske mål, vil truslene kunne ramme alle nivåer og samfunnsfunksjoner, men hvor den samlede/akkumulerte effekten over tid bygger opp under de strategiske målene. En trusselaktør kan derfor designe en kampanje som rammer én eller flere sektorer, for eksempel forsvarssektoren. Et delmål her kan være å ramme Forsvarets operative evne gjennom å påvirke faktorer og avhengigheter som understøtter denne. For eksempel gjennomføring av allierte øvelser, kommunikasjonssystemer og logistikk.

I det følgende nevnes noen typiske egenskaper ved sammensatte trusler som bidrar til å gjøre dem krevende å oppdage, forebygge og håndtere.

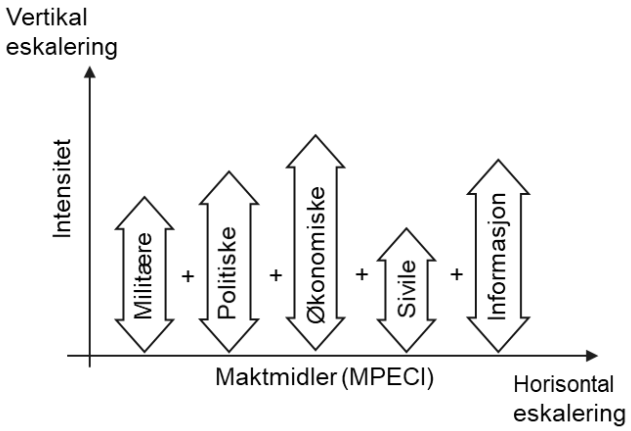
Kortsiktige og langsiktige mål: En trusselaktør kan ha både kortsiktige og langsiktige mål. Kortsiktig mål kan eksempelvis være knyttet til å påvirke et valg i en ønsket retning eller stoppe/forhindre militær øvelsesvirksomhet i bestemte områder. De kortsiktige målene henger ofte sammen med og forsterkes av aktiviteter for å nå mer langsiktige mål som for eksempel å øke egen innflytelse, skape sympati for egne krav og sikre egen suverenitet og handlefrihet.

Fokuserte (*spesifikke*) *og diffuse angrepsmål* (Pettyjohn & Wasser, 2019): Fokuserte/spesifikke mål angripes ofte for å oppnå mer kortsiktige mål og effekter. Eksempler på fokuserte angrepsmål er ekom[12]-systemer, kraftforsyning og spesifikke interessegrupper. Diffuse

[11] I (Grunnan, Endregard, Siedler og Elstad, 2020) diskuteres erfaringer fra øvelse Trident Juncture 2018 rundt samfunns- og statssikkerhet og totalforsvaret.
[12] Elektronisk kommunikasjon.

angrepsmål knyttes ofte til mer langsiktig rutinemessig påvirkning, som for eksempel spredning av propaganda og desinformasjon.

Vertikal og horisontal eskalering/de-eskalering: En trusselaktør kan eskalere/de-eskalere vertikalt ved å øke eller senke intensiteten på et gitt maktmiddel, eller eskalere/de-eskalere horisontalt ved å ta i bruk flere typer maktmidler innenfor MPECI. Ved lav intensitet kan det være hensiktsmessig å synkronisere bruk av flere maktmidler og holde intensiteten på et lavt nivå for å vanskeliggjøre deteksjon, identifikasjon og respons. MCDC (Cullen & Reichborn-Kjennerud, 2017) omtaler evnen til å kunne kontrollere horisontal og vertikal eskalering/de-eskalering, se Figur 2.2. Denne evnen gjør trusselen adaptiv og skalerbar.



Figur 2.2 Horisontal og vertikal eskalering ved bruk av ulike maktmidler. Figuren er hentet fra MCDC CHW I (Cullen & Reichborn-Kjennerud, 2017) og oversatt til norsk.

I tillegg er det vanlig å benytte kategoriene militære/ikke-militære og regulære/irregulære virkemidler.

Skjulte/fordekte og åpne trusler: En trusselaktør kan bruke både åpne og skjulte trusler, og kombinasjoner av disse. Ved å opptre skjult/fordekt vanskeliggjøres attribusjon, det vil si å avdekke hvem som står bak. Det kan derfor være vanskelig å finne entydig bevis for at en bestemt stat eller gruppe står bak et angrep. En trusselaktør vil kunne utnytte denne usikkerheten til å fornekte at de står bak. Trusler gjennom det digitale domenet øker mulighetene for å opptre fordekt.

Lovlige og ulovlige virkemidler: Lovlige virkemidler og effekten av disse, for eksempel innenfor det økonomiske domenet, kan utnyttes til å utøve press. De kan om ønskelig også kombineres med bruk av irregulære, ikke-lovlige virkemidler for å oppnå mål.

I et lengre tidsperspektiv kan aktører kombinere bruk av lovlig og ulovlige virkemidler for å tilrettelegge for senere angrep/kampanjer. Noen eksempler er å kombinere lovlig og ulovlig etterretningsvirksomhet for å avdekke sårbarheter i kritisk infrastruktur, og å utvikle sårbarheter

gjennom blant annet oppkjøp og investeringer i eiendom, infrastruktur og næringsliv. Slike oppkjøp gir både tilgang til informasjon og mulighet til å påvirke.

Strategisk kommunikasjon er normalt lovlig aktivitet som «alle» benytter for å fremme egne interesser og påvirke beslutningstakere.[13] Strategisk kommunikasjon er ikke bare avgrenset til bruk av tradisjonelle media og sosiale medier, men omfatter også for eksempel gjennomføring av militære øvelser (styrkemarkering) og andre virkemidler knyttet til MPECI.

Sammensatte trusler som har én eller flere av egenskapene nevnt i det foregående, bidrar til å skape usikkerhet og tvetydighet som utfordrer evnen til å oppdage, attribuere og forstå at man er utsatt for en kampanje/angrepspakke. Det vanskeliggjør også å identifisere og tolke/forstå en aktørs intensjon og målsetting. Samlet utfordrer dette å evnen til å oppnå nødvendig situasjons-forståelse som grunnlag for å kunne ta gode og tidsriktige beslutninger.

2.1.3 Sårbarheter og effekter

En sammensatt/hybrid trussel utgjør i utgangspunktet ingen risiko med mindre det finnes sårbarheter som kan utnyttes. Så hva gjør oss sårbare ovenfor sammensatte trusler?

Grunnleggende for arbeidet med å ivareta samfunns- og statssikkerhet er samfunnets kritiske funksjoner (DSB, 2017) og NATOs sju basiskrav til samfunnets funksjonalitet (FD, 2020, s.79). I DSB (2017) brytes samfunnsfunksjonene ned i tre hovedkategorier: styringsevne og suverenitet, befolkningens sikkerhet og samfunnets funksjonalitet. Sammensatte trusler kan påvirke funksjoner innen disse kategoriene både direkte og indirekte.

Det finnes mange sårbarheter i et samfunn som kan utnyttes av en trusselaktør. I MCDC relateres sårbarheter og effekter til PMESII-domenene (*political, military, economic, social, information, infrastructure*). En sammensatt trussel vil i tråd med begrepsforståelsen kunne ramme sårbarheter innen alle disse domenene. Eksempler kan være å utnytte politisk uenighet i bestemte saker, sårbarheter som påvirker forsvarets operative evne, sårbarheter i finans- og betalingssystemer, sårbarheter relatert til sosioøkonomiske og sosiokulturelle forhold (Diesen, 18), sårbarheter relatert til spredning av uriktig/falsk informasjon og sårbarheter i samfunns-kritisk infrastruktur.

Utviklingen har i de senere årene gått i retning av et mer komplekst samfunn med et økende antall aktører med roller innenfor samfunns- og statssikkerheten og økt grad av avhengighet mellom disse. Dette sammen med globalisering og digitalisering bidrar til å gjøre sårbarhets-bildet mer uoversiktlig. Et eksempel er Forsvarets avhengighet av enkelte kritiske samfunns-funksjoner. Disse funksjonene er igjen er avhengig av private leverandører av varer og tjenester, som igjen benytter utenlandske underleverandører. Dette gir lange og til dels uoversiktlige verdikjeder som gjør det vanskelig å ha full oversikt over sårbarheter og risiko i alle ledd.

[13] Fra Meld. St. 5: «Strategisk kommunikasjon kan beskrives som en statlig eller ikke-statlig aktørs planmessige og koordinerte bruk av alle kommunikative virkemidler for å fremme egne interesser og nå sine målsettinger».

Økt kompleksitet gjør at effekten av et angrep mot et gitt mål (direkte effekt) lettere sprer seg og kan få følgekonsekvenser for andre funksjoner og systemer som er avhengig av dette (indirekte effekter). Den akkumulerte effekten av direkte og indirekte effekter kan videre ha konsekvenser for statssikkerheten. Men kompleksitet er ikke nødvendigvis bare forbundet med økt sårbarhet. Kompleksitet kan også føre til økt robusthet og motstandsdyktighet (resiliens) fordi i et system med mange aktører kan flere ha helt eller delvis overlappende funksjonalitet.

Den teknologiske utviklingen med økt digitalisering i samfunnet introduserer nye sårbarheter som kan ramme alt fra enkeltpersoner til viktige samfunnskritiske funksjoner. Et eksempel er utviklingen av *Internet of Things* (IoT) (Farsund mfl., 2020). Digitale angrep kjenner ingen landegrenser og gjør det mulig å påvirke uten å gå til direkte fysisk angrep.

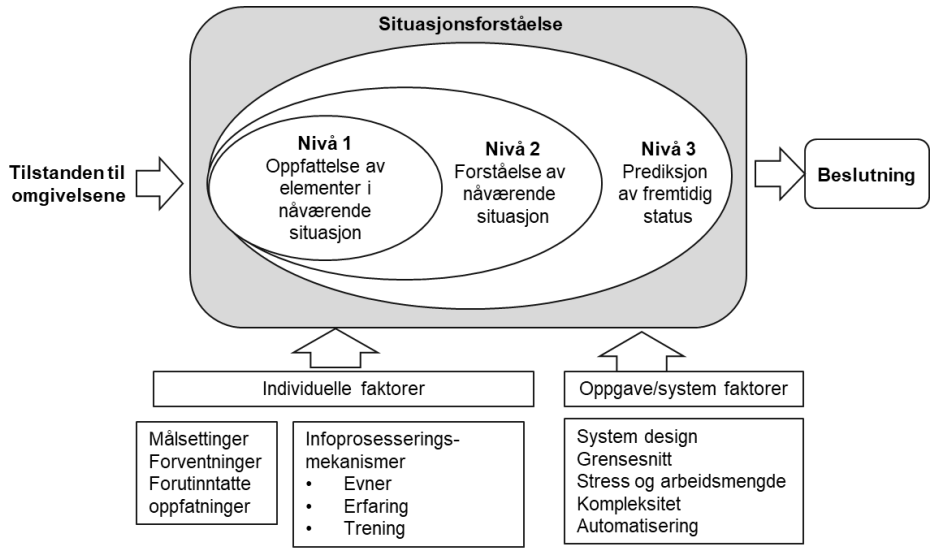
Sammensatte trusler er ofte assosiert med bruk av strategisk kommunikasjon, det vil si at en aktør ønsker påvirke beslutningstakere i en for seg gunstig retning (Stratcom CoE, 2019). Dette gjøres ved å benytte egnede kommunikative virkemidler for å spre informasjon (korrekt og/eller falsk) for å endre atferd og holdninger hos for eksempel befolkningen, politikere eller etniske, kulturelle og religiøse identitetsgrupper (JD, 2020, s.101). Økt digitalisering med massemedier, nettsider og sosiale medier gir flere kanaler for å drive strategisk kommunikasjon med tilgang til ulike målgrupper.

Langsiktig påvirkning kan tilrettelegge for senere eskalering blant annet gjennom utvikling og monitorering av sårbarheter over tid. Noen målsettinger kan være langsiktige, som for eksempel å endre holdninger (skape sympati for egne krav, skape splittelse) gjennom bruk av propaganda, spre desinformasjon og gi økonomisk støtte til bestemte interessegrupper. Dette kan være lovlige aktiviteter med lav intensitet som oppfattes som en del av normalsituasjonen, men som legger til rette for senere bruk av andre, mer direkte virkemidler.

Det kan være utfordrende å oppdage og forstå at enkelttrusler og uønskede hendelser spredt i tid og rom er en del av en planlagt kampanje. Sammensatte trusler utfordrer situasjonsforståelsen til både analytikere og beslutningstakere ved at de bidrar til usikkerhet og tvetydigheter rundt hva som er den faktiske situasjonen.

2.2 Situasjonsforståelse

Situasjonsforståelse er fundamentet for å kunne ta gode og rettidige beslutninger. En mye brukt modell for å forklare situasjonsforståelse er utviklet av Endsley (1995). Figur 2.3 viser en forenklet versjon av denne modellen, hvor situasjonsforståelsen deles inn i tre nivåer.



Figur 2.3 Endsleys modell for situasjonsforståelse (forenklet versjon).

Evnen til å oppnå situasjonsforståelse er individuell og avhenger av en rekke faktorer. Første nivå i modellen er å oppfatte elementer i omgivelsene i nåværende situasjon. Dette krever tilgang på relevant informasjon til rett tid om tilstanden til omgivelsene, for eksempel i form av et situasjonsbilde.

Neste nivå av situasjonsforståelse er å forstå elementenes betydning i nåværende situasjon ved å se sammenhengen mellom disse opp mot egne verdier, målsettinger og kontekst. Forståelsen vil i sterk grad påvirkes av individuelle faktorer som informasjonsprosesseringsevne som igjen avhenger av evner, trening og erfaring. I tillegg kan situasjonsforståelsen påvirkes av en rekke andre faktorer: forutinntatte meninger, forventninger, stress og hvordan informasjonen presenteres.

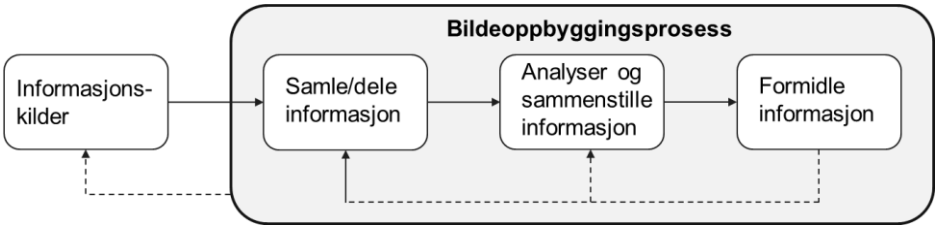
Det høyeste nivået av situasjonsforståelse er evnen til å kunne predikere elementenes fremtidige status. Å si noe sikkert om fremtidig status er ikke mulig. Men man kan gjøre vurderinger rundt mulige fremtidige situasjoner og hendelsesforløp ved bruk av for eksempel scenarioutvikling og -analyse og trendanalyser.

I det daglige og under krise og konflikt vil det foregå bildeoppbygging og beslutningstaking på ulike nivåer innen sektorene. For sammensatte trusler er det spesielt interessant hva som skjer relatert til samfunnskritiske funksjoner (DSB, 2017), inkludert Forsvaret. Ved uønskede hendelser som berører flere aktører snakkes det ofte om å oppnå en felles situasjonsforståelse for å kunne håndtere situasjonen. I henhold til Endsley (1995) vil involverte personer ha sin egen forståelse av situasjonen knyttet til egne oppgaver og funksjoner. Samtidig vil de også ha en felles forståelse relatert til felles oppgaver og funksjoner. Siden situasjonsforståelse er en individuell kognitiv egenskap, vil et mer dekkende begrep være koherent eller samstemt situasjonsforståelse.

Tilgang på relevant informasjon om omgivelsene er fundamentalt for å kunne oppnå god situasjonsforståelse. Ved å samle inn, analysere og sammenstille denne informasjonen bygger man situasjonsbilder tilpasset brukernes behov. Det bygges situasjonsbilder innen ulike sektorer og på ulike nivåer i staten. Innhold og detaljnivå vil variere alt etter hvilke informasjonsbehov man har.

2.2.1 Bildeoppbygging

Prosessen med å etablere og vedlikeholde situasjonsbildet refereres til som bildeoppbygging. Et eksempel på en bildeoppbyggingsprosessen er vist i Figur 2.4.[14]



Figur 2.4 Bildeoppbyggingsprosessen.

De viktigste aktivitetene i bildeoppbyggingsprosessen vist i Figur 2.4:

- *Samle og dele informasjon*: Evne til å motta og lagre informasjon som strømmer inn fra sensorer og informasjonskilder (*push*) og å etterspørre informasjon fra databaser og andre kilder (*pull*). Ofte baseres informasjonsinnsamlingen på et sett med parametere og indikatorer.

- *Analysere og sammenstille informasjon*: Evne til å analysere og sammenstille informasjon til et relevant situasjonsbilde. Dette innebærer evne til å filtrere, korrelere, aggregere og sammenstille relevant informasjon.

- *Formidle og presentere informasjon*: Evne til å presentere og formidle informasjon til mottakere i form av situasjonsbilder, og annen relevant informasjon som kan støtte opp under situasjonsforståelsen. Mottakere av situasjonsbildet kan for eksempel være analytikere eller beslutningstakere.

2.3 Situasjonsforståelse ved sammensatte trusler – utfordringer og behov

Sammensatte trusler utfordrer evnen til å etablere og vedlikeholde en bred situasjonsforståelse for å kunne forebygge og håndtere denne type trusler. For det første er det utfordrende å oppdage og forstå at man er utsatt for en planlagt kampanje/angrepspakke hvor trusler treffer ulike sektorer koordinert i tid og rom. Dernest å forstå hva som er angripers mål og intensjoner

[14] En annen måte å fremstille bildeoppbyggingsprosessen på er etterretningsprosessen som beskrevet i blant annet Forsvarets fellesoperative doktrine (FHS, 2019). Det finnes en beslutningstaker med et informasjonsbehov. Prosessen for å dekke dette behovet består av aktivitetene; styring av prosess, innhenting, bearbeiding og fordeling.

og hva vi kan forvente vil skje videre. Dette krever evne til å bygge relevante situasjonsbilder og produsere et hensiktsmessig beslutningsgrunnlag.

Sammensatte trusler har en rekke egenskaper som kan vanskeliggjøre situasjonsforståelse. Spesielt utfordrende er det i den lavere delen av konfliktspektret, i gråsonen mellom fred og krise, hvor det ikke er noen erklært konflikttilstand. I det daglige kan en trusselaktør utføre langsiktig påvirkning med eksempelvis bruk av politiske/diplomatiske, informasjonsmessige, økonomiske og juridiske virkemidler rettet mot mål i ulike sektorer. Intensiteten er lav og det benyttes ikke-voldelige virkemidler mot mer diffuse mål med lav kostnad og risiko for trusselaktøren. Denne type trusler representerer ofte små avvik fra normalsituasjonen og kan være vanskelig å oppdage. En enda større utfordring er å se enkelttrusler i sammenheng over tid og identifisere trusselaktørens mer langsiktige målsettinger og intensjoner. Vi må evne å forstå den akkumulerte effekten av disse truslene og hvilke konsekvenser dette kan ha for samfunns- og statssikkerheten.

I det daglige kan en fiendtlig aktørs virkemiddelbruk i hovedsak være lovlig, for eksempel i form av investeringer i virksomheter og eiendom, økonomisk støtte til spesielle interesse-grupper, bruk av media og diplomatiske/juridiske virkemidler. Virkemiddelbruken kan være spredd over flere sektorer. Målsettingen kan være å øke egen innflytelse og tilrettelegge for senere eskalering med bruk av eksempelvis mer voldelige virkemidler for å oppnå spesifikke mål. Virkemiddelbruken kan være åpen eller skjult (fordekt) og ha en intensitet som ligger under normale terskler for varsling og rapportering.

2.3.1 Identifiserte behov

Situasjonsforståelse ved sammensatte trusler bygges opp over tid og er en tverrsektoriell utfordring. Det er behov for et nasjonalt tverrsektorielt situasjonsbilde som inngår i beslutningsgrunnlaget som presenteres for beslutningstakere med ansvar og myndighet for forebygging og håndtering av denne type trusler.

Evne til å oppdage sammensatte trusler: For å oppdage bruk av sammensatte trusler må man evne å samle inn og dele relevant informasjon, også informasjon som ikke nødvendigvis er direkte relevant for en selv. Informasjonsinnsamling (pull) krever kunnskap om egne informasjonsbehov. Disse vil typisk være knyttet til trusler mot egen virksomhet, sårbarheter som kan utnyttes, uønskede hendelser og effekter/konsekvenser av disse på egen virksomhet og måloppnåelse. Videre kreves det kunnskap om hvor denne informasjonen kan finnes, det vil si kjennskap til relevante informasjonskilder innenfor både offentlig og privat sektor.

Informasjonsdeling følger push-prinsippet hvor en informasjonskilde velger å dele informasjon med én eller flere mottakere. Her må man forstå hverandres informasjonsbehov på tvers av sektorer og nivåer, og tilrettelegge for god horisontal og vertikal informasjonsflyt. Dette er spesielt utfordrende ved lav intensitet (små avvik fra normalsituasjonen), hvor trusler og effekter kan gå under normale terskler for varsling og rapportering. Terskelen må derfor være lav nok til at relevant informasjon rapporteres videre samtidig som man også må sørge for at mottaker ikke overbelastes med unødvendig informasjon. For å få til dette kreves en god

kjennskap informasjonsbehov og til hva som er normalsituasjonen innen ulike samfunns-områder og -funksjoner.

Videre er det behov for å kunne utveksle gradert informasjon mellom informasjonskilder og forskjellige mottakere. For å få til dette må man ivareta informasjonens konfidensialitet og integritet. Dette krever kunnskap, kompetanse og hensiktsmessige IKT-systemer for utveksling av informasjon på ulike graderingsnivåer.

Sist, men ikke minst, er informasjonsdeling avhengig av tillit mellom aktørene. Det må utvikles en delingskultur hvor man beveger seg bort fra «*need-to-know*» over mot «*responsibility-to-share*». For å få til dette må det også finnes et hensiktsmessig lov- og hjemmelsgrunnlag som tilrettelegger for deling av informasjon.

Evne til å forstå at man er utsatt for sammensatte trusler: For å kunne bygge og vedlikeholde et relevant situasjonsbilde og utvikle et godt beslutningsgrunnlag, er det behov for å kunne identifisere og attribuere trusler og sette trusler og hendelser inn i kontekst.

En kampanje med sammensatte trusler bruker forskjellige maktmidler mot sårbarheter i ulike deler av samfunnet for å nå kortsiktige og langsiktige mål. Trusler og effekter kan være spredt i tid og rom (ulike sektorer, ulike nivåer og ulike geografiske lokasjoner). Dette utfordrer evnen til å se uønskede hendelser i sammenheng og forstå den akkumulerte effekten av disse, på tvers av sektorer opp mot viktige mål og verdier relatert til samfunns- og statssikkerheten. For å styrke denne evnen, er det behov for god kjennskap til egne verdier som vi vil beskytte, og sårbarheter/svakheter som kan utnyttes av en trusselaktør for å ramme disse («kjenn deg selv»). Tilsvarende er det behov for god kunnskap mulige trusselaktører («kjenn din fiende»).

I en kampanje med sammensatte trusler kan trusselaktøren opptre både åpent og fordekt. Fordekte trusler utfordrer evnen til å fastslå hvem som står bak et angrep (attribusjon). Denne usikkerheten kan utnyttes av trusselaktøren til å benekte at de står bak. Attribusjon av trusler er viktig informasjon i et situasjonsbilde og en sentral del av et beslutningsgrunnlag.

Det er utfordrende å oppdage at man er utsatt for en kampanje/angrepspakke med bruk av sammensatte trusler. Like viktig er det å kunne avkrefte mistanke om bruk av denne type trusler. Er det snakk om uavhengige hendelser, eller er det en sammenheng mellom disse? Utnytter trusselaktøren oppdukkende sårbarheter/muligheter, eller er truslene en del av en planlagt kampanje? Har hendelsene en akkumulert effekt på, for oss, viktige verdier og mål? Og er dette i tråd med antatte målsettinger hos en trusselaktør? Er det et utslag av normal negativ samhandling fra en aktør, eller ligger det noe mer alvorlig bak? For å kunne gi gode svar på disse spørsmålene, er det behov for en analysekapasitet støttet av et nettverk bestående av personer med inngående kunnskap om trusselaktører, sårbarheter og effekter, og evne til å kunne se dette i en tverssektoriell sammenheng.

Et beslutningsgrunnlag er mer enn et situasjonsbilde. Det skal støtte alle nivåene i Endsleys modell av situasjonsforståelse. Det bør derfor også inneholde en fremskriving av situasjonen,

det vil si vurderinger av hva som kan skje videre i et kortere og lengre tidsperspektiv, en vurdering av risiko og forslag til tiltak for å forebygge og håndtere trusler.

Evne til å formidle situasjonsbilde og beslutningsgrunnlag: Beslutningsgrunnlaget med situasjonsbilde må dekke beslutningstakernes informasjonsbehov i så stor grad som mulig og formidles på en måte som understøtter beslutningstakernes situasjonsforståelse. For å få til dette, er det nyttig å kartlegge og formulere informasjonsbehov og se på mulige måter å fremstille beslutningsgrunnlaget på gjennom for eksempel spill og scenariodiskusjoner.

3 Forutsetninger og rammebetingelser for utviklingen av et konsept

En sentral anbefaling fra MCDC (Monaghan mfl., 2019) er å utnytte, tilpasse og forsterke eksisterende institusjoner, prosesser og organisasjoner der dette er hensiktsmessig. Et fremtidig konsept for å understøtte situasjonsforståelse vil blant annet måtte ta utgangspunkt i dagens system for krisehåndtering. Det er derfor behov for å gi en kortfattet oversikt over dagens prosesser, struktur og organisasjon for nasjonal krisehåndtering. I tillegg vil vi trekke frem andre nasjonale forutsetninger og rammer som også vil påvirke evnen til å oppnå situasjons-forståelse, slik som befolkningen og lovverk.

Dette kapitlet tar ikke mål av seg å gi noen fullstendig oversikt over prosesser og organisasjon, med alle roller, ansvar og myndighet forbundet med krisehåndtering. I stedet trekker vi frem det som anses mest relevant med hensyn til situasjonsforståelse rundt sammensatte trusler.

3.1 Nasjonal krisehåndtering

Det nåværende systemet for nasjonal krisehåndtering vil være utgangspunktet for å forsterke evnen til å oppdage og håndtere sammensatte trusler. Noen sentrale dokumenter er Instruks for departementenes arbeid med samfunnssikkerhet (2017)[15], Meld. St. 5 (2020–2021) (JD, 2020) og Støtte og samarbeid (FD/JD, 2018).

I Norge følger beredskap og krisehåndtering fire grunnleggende prinsipper: *ansvarsprinsippet*, *likhetsprinsippet*, *nærhetsprinsippet* og *samvirkeprinsippet*. Effekten av dette er at det i stor grad er de enkelte departementene med underliggende direktorater og etater som har ansvaret for forebygging, beredskap og håndtering innenfor sine sektorer. I tillegg har kommunene og fylkene (regionene) ansvar for planlegging og krisehåndtering i kommunene og på tvers av kommunegrenser. Nasjonalt beredskapssystem består av Beredskapssystem for forsvarssektoren

[15] Samfunnssikkerhetsinstruksen: https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349

(BFF) og Sivilt beredskapssystem (SBS). Disse dokumentene beskriver tiltak og ansvar i forbindelse med heving av beredskap og krisehåndtering.

Det bygges situasjonsbilder på ulike nivåer innen samfunnssektorene, blant annet for å støtte håndtering av uønskede hendelser som rammer samfunnets kritiske funksjoner (DSB, 2017). Det er etablert situasjonssentre i en rekke etater, direktorater og departementer som bygger egne situasjonsbilder, basert på innsamlet informasjon og informasjon som blant annet deles over samordnings- og fagkanal.[16]

Sektorene, kommuner og fylker er pålagt å gjennomføre risiko- og sårbarhetsanalyser (ROS). ROS-analysene tar for seg ulike typer uønskede hendelser som kan påvirke evnen til å opprett-holde samfunnskritiske funksjoner og få konsekvenser for samfunnsverdier som: liv og helse, stabilitet, natur og miljø og materielle verdier. Truslene kan være større ulykker, naturkata-strofer og intenderte handlinger. En helhetlig ROS-analyse vurderer uønskede hendelser med utgangspunkt i årsaker og sannsynlighet, sårbarheter, konsekvenser og usikkerhet (DSB, 2014).

Det finnes derfor informasjon om sårbarheter og mulige konsekvenser av disse. Denne informasjonen kan utnyttes i arbeidet med å utvikle indikatorer for å oppdage sammensatte trusler og effekter/konsekvenser av disse. I tillegg gjennomføres det ROS-analyser på nasjonalt nivå i regi av DSB, se for eksempel Analyse av krisescenarioer 2019 (DSB, 2019). En mulig mangel ved disse analysene er at de først og fremst vektlegger større ulykker og naturhendelser, og i mindre grad intenderte sammensatte tusler.[17]

3.1.1 Sentrale aktører

Hvilke prosesser og mekanismer finnes hos sentrale aktører som kan støtte bildeoppbygging og situasjonsforståelse? Denne beskrivelsen er i hovedsak basert på Instruks for departementenes arbeid med samfunnssikkerhet (JD, 2017) og stortingsmeldingen Støtte og samarbeid (FD/JD, 2018).

3.1.1.1 Politisk strategisk nivå

Regjeringen er øverste ansvarlige for beredskap og krisehåndtering. Regjeringens sikkerhets-utvalg (RSU) behandler i hovedsak saker som er av forsvarsmessig eller sikkerhetspolitisk karakter. Ansvaret for forebygging, beredskapsforberedelser og kompetanse er i stor grad tillagt de ulike fagdepartementene og deres underliggende etater og kommuner og fylker/regioner.

Justis- og beredskapsdepartementet (JD) er fast lederdepartement og har samordningsansvar ved sivile kriser hvis ikke annet er bestemt. Forsvarsdepartementet (FD) og Utenriksdepartementet (UD) får større rolle og ansvar ved sikkerhetspolitiske kriser og konflikter. Lederdepartementet har ansvar for håndtering og koordinering av kriser på departementsnivå som blant annet

[16] DSBs retningslinjer for varsling og rapportering på samordningskanal: https://www.dsb.no/lover/risiko-sarbarhet-og-beredskap/andre-dok/retningslinjer-for-varsling-og-rapportering-pa-samordningskanal/
[17] DSB har gjennomført en risikoanalyse av et hybrid angrep mot Norge, som er dokumentert i en gradert rapport.

innebærer å innhente og bearbeide informasjon, utarbeide situasjonsrapporter og beslutningsgrunnlag og sørge for informasjon til media og befolkning.

JD har samordningsansvaret for samfunnssikkerhetsarbeidet, mens ansvar innenfor de enkelte kritiske samfunnsfunksjonene er tillagt forskjellige departementer. Dette inkluderer også ansvaret for å gjennomføre ROS-analyser med oversikt over viktige sårbarheter.

Kriserådet er det øverste administrative koordineringsorganet på departementsnivå, og ble opprettet for å styrke den sentrale, tverssektorielle koordineringen ved kriser. Rådet har seks faste medlemmer, men kan utvides ved behov. Alle departementer kan ta initiativ til å kalle inn Kriserådet (JD, 2020, s.167).

Krisestøtteeneheten (KSE) er organisert under JD. Sivilt situasjonssenter er en del av KSE og er fast kontaktpunkt for informasjon til og fra JD ved større hendelser og kriser. KSE skal bidra til rettidig varsling og analyse av situasjonsbilde. KSE og sivilt situasjonssenter skal yte støtte til lederdepartementet og Kriserådet, se Samfunnssikkerhetsinstruksen (2017).

3.1.1.2 Direktorater og etater

Hensikten her er ikke å gi en uttømmende oversikt over etatene innenfor statsforvaltningen, men å nevne de etatene som kan tenkes å ha en sentral rolle i forbindelse med å oppdage og håndtere sammensatte trusler.

Etterretnings- og sikkerhetstjenestene (EOS):
EOS-tjenestene har en sentral rolle i forbindelse med å oppdage og vurdere trusler innen alle domener.

Etterretningstjenesten (E-tjenesten) er en del av Forsvaret og har som viktigste oppgave å samle inn informasjon om utenlandske forhold som kan true Norge og norske interesser. E-tjenesten støtter sivile norske myndigheter med informasjon om og vurderinger av utenriks-, sikkerhets- og forsvarspolitiske forhold.[18]

Politiets sikkerhetstjeneste (PST) er direkte underlagt JD og har som sine viktigste oppgaver å forebygge og etterforske straffbare handlinger mot rikets sikkerhet.[19]

Nasjonal sikkerhetsmyndighet (NSM) er administrativt underlagt JD.[20] NSM har tilsynsmyndighet og fagmyndighet innenfor forebyggende sikkerhet i henhold til sikkerhetsloven. NSM skal ha helhetlig oversikt over IKT-risikobilde og har viktige oppgaver innen IKT-sikkerhet og ansvar for å koordinere håndtering av cyberhendelser mot samfunnskritisk infrastruktur. NSM drifter nasjonalt varslingssystem for digital infrastruktur (VDI). De er også en del av Felles cyberkoordineringssenter (FCKS) for felles koordinering ved cyberhendelser.

[18] https://www.forsvaret.no/om-forsvaret/organisasjon/etterretningstjenesten
[19] https://www.pst.no/temasider/oppgaver/
[20] https://nsm.no/getfile.php/134519-1606830131/Demo/Dokumenter/instruks-for-nsm.pdfs

Det er etablert ulike samarbeidsfora på tvers av tjenestene, blant annet innen kontraterror og cyberhendelser.

Forsvaret:
Forsvarets hovedoppgaver er rettet inn mot å ivareta statssikkerheten. I det daglige løser Forsvaret fredstidsoppgaver, yter støtte til sivil sektor og driver forberedelser (planlegging, trening og øving) for å kunne møte kriser og konflikt. En av Forsvarets oppgaver er å sikre et godt nasjonalt beslutningsgrunnlag for politisk ledelse og Forsvarets øverste ledelse.

Forsvaret har flere situasjonssentre på ulike nivåer (militær-strategisk, operasjonelt og taktisk nivå) i organisasjonen som driver informasjonsinnsamling (overvåkning) og bildeoppbygging rundt aktiviteter og hendelser i norske interesseområder. FOH har ansvaret for å samle og sammenstille informasjon fra taktisk nivå til et fellesoperativt situasjonsbilde. Dette bildet er gradert og inneholder blant annet informasjon om egen og utenlandsk militær aktivitet i våre interesseområder. FOH mottar også informasjon fra ulike sivile aktører og har liaisoner fra aktører i totalforsvaret

Heimevernet (HV) har lokalt territorielt ansvar og er i det daglige et viktig bindeledd mellom Forsvaret og det sivile samfunn. HVs distriktssjefer ivaretar den daglige koordineringen og sivilt-militært samarbeid med kommuner, regioner og sivile aktører på vegne av sjef FOH.

Forvaret har egne graderte IKT-systemer for informasjonsdeling og bildeoppbygging.

Totalforsvaret:
Totalforsvaret er ingen egen organisasjon eller et forvaltningsnivå, men et sett av prosedyrer for samhandling mellom aktører med roller innenfor samfunns- og statssikkerhet. Dokumentet Støtte og samarbeid (FD/JD, 2018) gir en beskrivelse av totalforsvaret i dag. Her står det at totalforsvarskonseptet skal sikre best mulig utnyttelse av samfunnets begrensede ressurser når det gjelder forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespektret (FD/JD, 2018, s. 15). Totalforsvaret er et gjensidig samarbeid mellom sivile og militære aktører knyttet til kriser i fred og under væpnet konflikt. Innenfor rammene av totalforsvaret er det etablert en rekke fora for samarbeid og koordinering på sentralt, regionalt og lokalt nivå. Disse kan ha en rådgivende funksjon eller operativ funksjon. I (FD/JD, 2018) beskrives fora og organer som er viktige for informasjonsutveksling i totalforsvaret. I «Norsk vertslandsstøttekonsept til bruk i totalforsvaret» (FOH, 2018, s. 7) vises en prinsippskisse for hvordan et operasjonelt totalforsvarsbilde kan etableres basert blant annet på militære og etats-vise situasjonsbilder for å støtte «felles» situasjonsforståelse ved forberedelser til og gjennom-føring av alliert mottak.

Justissektoren:
Justis- og beredskapsdepartementet (JD) og justissektoren har i utgangspunktet samordnings-ansvaret for krisehåndtering i fredstid. Politidirektoratet (POD) er det øverste ledelsesnivå i politiet med ansvar for faglig ledelse, styring, oppfølging og utvikling av politidistriktene og særorganene i politiet. Politidistriktene leverer polititjenester og har egne operasjonssentraler. Viktige særorganer er Kripos og Økokrim. Kripos er nasjonal enhet for bekjempelse av

organisert og annen kriminalitet, og driver blant annet Nasjonalt cyberkrimsenter. Økokrim er den sentrale enheten for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet.

Direktoratet for sivil beredskap (DSB): DSB har en sentral rolle innen samfunnssikkerhets-arbeidet og understøtter JD med hensyn til samordning av aktører. DSB bistår også JD med tilsyn av de andre departementenes samfunnssikkerhetsarbeid som blant annet innebærer å følge opp ROS-analyser innenfor ulike sektorer.

DSB har også ansvar for samordningskanalen for deling av informasjon.[21] Det er to hovedlinjer for varsling og rapportering: Samordningskanalen benyttes til formidling av mer sektorover-gripende informasjon fra kommuner til fylke og videre til DSB og til sivilt situasjonssenter i KSE. Fagkanalen er til for utveksling av mer sektorspesifikk informasjon fra lokal fagetat via regionale og sentrale fagetater til fagdepartement. Det er også lagt til rette for horisontal informasjonsflyt mellom kanalene på ulike nivåer. Uønskede hendelser av en viss størrelse varsles eller rapporters på samordningskanal/fagkanal.

DSB-CIM[22] er et web-basert krisehåndteringssystem. Verktøyet brukes til informasjonsdeling, varsling og mobilisering ved ulykker og uønskede hendelser.

Kommuner og fylker:
Statsforvalter (tidligere Fylkesmann) har regionalt samordningsansvar innen samfunnssikkerhet. Blant annet skal de ha oversikt over risiko- og sårbarheter i fylke/region – fylkesROS. De har en samordningsrolle innenfor totalforsvaret og leder fylkesberedskapsrådet. Fylkesberedskapsrådet har en operativ funksjon ved at de skal sørge for koordinering og samordning ved uønskede hendelser.

Uønskede hendelser rammer ofte i en kommune. Kommunene har ansvar for krisehåndtering i kommunen og skal gjennomføre ROS-analyser for å kartlegge sårbarheter og uønskede hendelser som kan ramme kommunen.

Privat sektor:
Privat sektor er involvert i leveranser av varer og tjenester knyttet til de samfunnskritiske funksjonene. Blant annet leverer de transport- og ekom-tjenester og står for forsyning av elektrisk kraft. I denne sammenheng er de eiere av kritisk infrastruktur.

[21] DSBs retningslinjer for rapportering og varsling på samordningskanal: https://www.dsb.no/lover/risiko-sarbarhet-og-beredskap/andre-dok/retningslinjer-for-varsling-og-rapportering-pa-samordningskanal/
[22] DSB Crisis information management (CIM). For mer informasjon se for eksempel: https://www.fylkesmannen.no/Nordland/Samfunnssikkerhet-og-beredskap/DSB-CIM/Veiledningsmateriell-for-DSB-CIM/

3.2 Befolkning

Under workshop 1 i november 2019 (se kapittel 1.2) ble befolkningen fremhevet som en viktig ressurs og aktør, både som informasjonskilde og som mål for påvirkning ved bruk av sammensatte trusler.

I RAND-rapport (Pettyjohn & Wasser, 2019) trekkes faktorer som tillit til hverandre, tillit til myndigheter, utdannelse, fri presse og demokratiske tradisjoner frem som viktige for samfunnets evne til å motstå sammensatte trusler, spesielt trusler rettet mot å påvirke befolkningens meninger og holdninger. Det norske samfunnet er i utgangspunktet godt stilt med hensyn til disse faktorene. Vi har høy grad av tillit til myndighetene, et generelt høyt kunnskapsnivå i befolkningen og ingen store/dominerende interessegrupper. Det legges også vekt på kildekritikk allerede tidlig i utdanningsløpet. Samlet bidrar dette til å minke sårbarheten (øke motstandsdyktigheten) ovenfor falske nyheter og påvirkning.

3.3 Lover og hjemmelsgrunnlag

Informasjonsinnsamling og bildeoppbygging må forholde seg til eksisterende lover og hjemmelsgrunnlag. Hvilke muligheter og begrensninger ligger her?

Som beskrevet i kapittel 2 kan sammensatte trusler bestå av både lovlige og ulovlige virkemidler. For å kunne oppdage og se ulike hendelser i sammenheng er man avhengig av å kunne samle inn informasjon om både ulovlig og lovlig virksomhet. I hvilken grad åpner lovverket for å samle inn informasjon om lovlig virksomhet, som for eksempel oppkjøp av eiendom og investeringer i virksomhet og infrastruktur?

Situasjonsforståelse rundt sammensatte trusler betinger god informasjonsflyt mellom ulike sektorer og nivåer, kommune, fylke og private aktører. I hvilken grad har vi et hensiktsmessig lov- og hjemmelsgrunnlag som tillater og oppmuntrer til nødvendig informasjonsdeling i møte med sammensatte trusler?

4 Situasjonsbilder og beslutningsgrunnlag

I dette kapitlet søker vi å svare på utfordringene og behovene som ble identifisert i kapittel 2, gjennom å trekke frem og diskutere prinsipper og mulige løsninger for hvordan man kan understøtte situasjonsforståelse i møte med sammensatte trusler.

For å bygge et relevant bilde må man ha evne til å samle inn, analysere og sammenstille informasjon til et situasjonsbilde tilpasset den eller de beslutningsprosessene som skal støttes. I

det videre vil vi skille mellom roller som har ulike oppgaver og informasjonsbehov: informasjonskilde, analytiker og beslutningstaker. Informasjonskildene deler informasjon om trusler og effekter med analytikere. Analytikerne analyserer og setter informasjonen sammen til et situasjonsbilde og beslutningsgrunnlag som igjen presenteres for beslutningstakere for å understøtte deres situasjonsforståelse. Dette er illustrert i Figur 4.1

Figur 4.1 Roller og oppgaver relatert til situasjonsforståelse i møte med sammensatte trusler.

4.1 Etablere tverrsektorielt situasjonsbilde

Behovet for et tverrsektorielt situasjonsbilde er forklart i kapittel 2.3. Behovet understrekes også i samfunnssikkerhetsmeldingen (JD, 2020) og i langtidsplan for forsvarssektoren (FD, 2020) i forbindelse med videreutvikling av sivilt-militært samarbeid og totalforsvaret.

Et situasjonsbilde kan forstås som summen av informasjon om elementer i omgivelsene som har relevans for beslutningsprosessen som skal støttes. I dette ligger det at informasjonen i bildet er filtrert, analysert og tolket. Situasjonsbildet vil typisk være deskriptivt og gi oversikt over nåværende situasjon rundt trusler, uønskede hendelser og tilstanden til samfunnskritiske funksjoner. Bildet kan også inneholde status for egne kapasiteter og historikk. Kvaliteten på situasjonsbildet vil avhenge av hvor relevant det er for beslutningsprosessene det skal støtte. Relevans avhenger blant annet av hvor komplett og korrekt situasjonsbildet er med hensyn til å gjengi relevante elementer i nåværende situasjon.

Et tverrsektorielt situasjonsbilde skal understøtte situasjonsforståelse i møte med sammensatte trusler. Det vil si at det skal inneholde informasjon som bidrar til at man oppdager og gjenkjenner sammensatte trusler som rammer innen ulike samfunnssektorer. Det er typisk behov for informasjon om trusler, sårbarheter, uønskede hendelser og effekter på samfunnet for å få oversikt over situasjon, og kunne oppdage avvik fra det som er normalt.

For å kunne bygge og vedlikeholde et tverrsektorielt situasjonsbilde, må man ha tilgang på informasjon fra ulike kilder på tvers av sektorer og nivåer. Det bygges i dag situasjonsbilder på flere nivåer innen sektorene – både militære og sivile. Disse er normalt mer avgrensede og fagspesifikke. Et situasjonsbilde som skal understøtte situasjonsforståelse rundt sammensatte trusler, må kunne dekke alle sektorer med ansvar for kritiske samfunnsfunksjoner som kan ha betydning for statssikkerheten. Et slikt tverrsektorielt situasjonsbilde kan bygge på informasjon fra sektorvise bilder, sammen med informasjon fra andre relevante kilder. Et interessant spørsmål er i hvilken grad dagens krisehåndteringssystem i tilstrekkelig grad støtter opp under dette. Innen totalforsvaret er det etablert mange tverrsektorielle fora og grupper for gjensidig

informasjonsutveksling (FD/JD, 2018). Disse kan muligens utnyttes bedre for å understøtte informasjonsutveksling rundt sammensatte trusler.

Bildet kan presenteres på ulike måter ved bruk av ulike verktøy – fra muntlige og tekstlige fremstillinger til bruk av grafiske display (dashbord).

4.2 Utarbeide beslutningsgrunnlag

Et situasjonsbilde skal støtte opp under god situasjonsforståelse hos både analytikere og beslutningstakere. Analytikernes oppgave er å bygge et tverrsektorielt situasjonsbilde og frembringe et solid beslutningsgrunnlag. Dette må videre presenteres for beslutningstakerne på en måte som understøtter god situasjonsforståelse og som vekker tillit og troverdighet.

Et godt beslutningsgrunnlag svarer på beslutningstakernes informasjonsbehov. Et oppdatert situasjonsbilde er en viktig del av et beslutningsgrunnlag, men er ikke alene tilstrekkelig for å understøtte god situasjonsforståelse. I henhold til Endsley (1995) må man også ha med en fremskriving av nåværende situasjon, det vil si en vurdering av mulige fremtidige utviklingsløp. En vanlig metode for dette er å utvikle scenarioer som beskriver ulike plausible fremtidssituasjoner, basert på vurderinger av trusselaktørenes mål, intensjoner og evner. Videre bør beslutningsgrunnlaget inneholde risikovurderinger rundt kritiske sårbarheter og mulige effekter og konsekvenser på kort og lengre sikt. Beslutningsgrunnlaget bør også presentere hypoteser om mulig påvirkning av sammensatte trusler, sammen med en vurdering av de viktigste argumentene for og imot deres gyldighet. Det er også vanlig at et beslutningsgrunnlag inneholder forslag til tiltak/handlemåter for å imøtegå trusselen med en vurdering av fordeler og ulemper.

4.3 Samle og dele informasjon

Evnen til å samle inn og dele informasjon er grunnleggende for å kunne etablere og vedlikeholde situasjonsbilder og produsere et relevant beslutningsgrunnlag. I kapittel 2.3 er det identifisert en rekke utfordringer og behov knyttet til innsamling og deling av informasjon rundt sammensatte trusler, spesielt sammensatte trusler i den lavere delen av konfliktspekteret – gråsonen.

4.3.1 Informasjonsflyt

I all kommunikasjon er det én avsender (kilde) og én eller flere mottakere av informasjonen. Informasjonen kan deles ved at den sendes til mottaker i henhold til gitte kriterier for informasjonsdeling (push-prinsipp), eller informasjonen kan etterspørres av mottaker (pull-prinsipp) for å dekke spesifikke informasjonsbehov. Begge disse prinsippene er relevante i bildeoppbyggingsprosessen.

4.3.1.1 Kartlegge informasjonsbehov

Grunnleggende for god informasjonsflyt er forståelse for egne og andres informasjonsbehov, og forståelse av andre aktørers oppdrag og funksjoner. Som beskrevet i kapittel 2.3 vil sammensatte trusler sannsynligvis øke behovet for å utveksle informasjon om trusler og effekter på tvers av samfunnssektorene. Informasjonen må også utveksles med nasjonalt strategisk nivå som har ansvar for å koordinere og beslutte tiltak for å forebygge og håndtere trusler mot samfunns- og statssikkerheten (FD/JD, 2018).

For å kartlegge egne informasjonsbehov, er det nødvendig å kjenne til egne verdier og sårbarheter og hvilke trusselaktører som kan tenkes å utfordre oss. Risiko- og sårbarhetsanalyse (ROS) er en metode som kan hjelpe til med å utlede informasjonsbehov på tvers av sektorer og nivåer (DSB, 2014, Rausand & Utne, 2011). Her finnes det allerede analyser innenfor de ulike sektorene som kan benyttes. Utover dette er det behov for å gjennomføre tverrsektorielle ROS-analyser med fokus på sammensatte trusler. Informasjonsbehov kan uttrykkes ved å benytte indikatorer, som beskrives i kapittel 4.3.2. Det finnes også flere andre metoder og teknikker for å utvikle og strukturere informasjonsbehov, blant annet ulike problemstrukturerende metoder, se for eksempel (NATO, 2017a).

I forbindelse med å kartlegge informasjonsbehov er det behov for å se på hvilke muligheter og begrensinger som gjelder for informasjonsdeling. Et eksempel på spørsmål som bør utredes er om Norge i dag har et hensiktsmessig lov- og hjemmelsgrunnlag som gjør det mulig for organisasjoner med ansvar for samfunns- og statssikkerhet å innhente og dele relevant informasjon. Dette kan være informasjon om trusler, sårbarheter og effekter som rammer på tvers av ansvarsområder og sektorer. I Finland har de tilpasset lovverket for å styrke hjemmelsgrunnlaget for innsamling og deling av etterretningsinformasjon som vedrører trusler mot statssikkerheten (Ferm mfl., 2018).

4.3.1.2 Push og pull

Push-prinsippet krever kjennskap til mottakernes informasjonsbehov. Som nevnt i kapittel 2 vil sammensatte trusler sannsynligvis medføre et økt informasjonsbehov sammenliknet med det som er normalt ved vanlig krisehåndtering i henhold til krisehåndteringsprinsippene. Spesielt gjelder dette mottakere på operasjonelt og strategisk nivå, som har behov for å kunne se trusler, uønskede hendelser og effekter i sammenheng på tvers av sektorer og nivåer. Type og mengde informasjon som er aktuelt å dele vil øke hvis en trusselaktør utnytter bredden av trusler innenfor MPECI til å ramme sårbarheter innenfor flere av PMESII-domenene. Trusler, og direkte og indirekte effekter av disse, kan forplante seg fra lavt nivå i sektorene og kommunene til samlet å kunne true samfunns- og statssikkerheten.

Et konsept for å bedre situasjonsforståelsen i møte med sammensatte trusler bør derfor inkludere tiltak for å sikre god horisontal og vertikal informasjonsflyt og som understøtter både push og pull av informasjon. En forutsetning for dette er god oversikt og kunnskap over egne og andre aktørers informasjonsbehov, og at terskelen for å varsle og rapportere avvik fra normalsituasjonen er lav nok til at lavintensitets sammensatte trusler oppdages.

Private aktører med rolle innenfor samfunns- og statssikkerhet kan også være mål for sammensatte trusler. Det er derfor behov for å etablere mekanismer for informasjonsdeling med privat sektor. Dette finnes i dag samarbeidsorganer innenfor rammene av totalforsvaret, men det bør vurderes om dette i tilstrekkelig grad dekker behovene for informasjonsdeling rundt sammensatte trusler. Mekanismer for informasjonsdeling inkluderer prosesser, prosedyrer og hensiktsmessige teknologiske løsninger (IKT-systemer).

4.3.1.3 Terskler for varsling og rapportering

Trusler og uønskede hendelser håndteres normalt i sektorene i henhold til prinsippene om ansvar, nærhet, likhet og samvirke. Videre varsling og rapportering vil avhenge av omfang og alvorlighet av hendelsene og om disse vurderes å kunne ha konsekvenser for samfunns- og statssikkerheten. Det er derfor ikke gitt at mindre alvorlige hendelser som kan ha tverrsektoriell interesse rapporteres videre.

Sammensatte/hybride lavintensitetstrusler kan hver for seg være så små/ubetydelige at man risikerer at de går under normale deteksjons- og varslingsterskler. Intensitet kan bety både alvorlighetsgrad av truslene og hyppighet. En motstander med god kjennskap til våre rutiner og sårbarheter vil kunne justere trusselen vertikalt (høyere intensitet) eller horisontalt (involvere flere maktmidler innen MPECI), slik at enkelthendelser ligger under normale terskler for rapportering og varsling (mindre avvik fra normalsituasjonen). Terskelen for å varsle og rapportere må derfor være lav nok til at selv lavintensitetstrusler og –hendelser, som kan ha tverrsektorielle konsekvenser, rapporteres videre til berørte sektorer og til høyere nivå. En enkelt hendelse innenfor en sektor, kan i det større bildet være en brikke i en planlagt kampanje fra en motstander for å nå mer overordnede og langsiktige mål som kan true vår statssikkerhet.

Det å forstå normalsituasjonen er grunnleggende for å kunne detektere avvik som kan ha konsekvenser utover egen sektor. Kjennskap til normalsituasjonen finnes i de ulike sektorene, men må også deles.

Videre bør man vurdere om sektorprinsippet og krisehåndteringsprinsippene i tilstrekkelig grad understøtter informasjonsdeling for å oppnå situasjonsforståelse rundt sammensatte trusler. I hvilken grad tilrettelegger prinsippene for informasjonsflyt mellom sektorene og til høyere myndighetsnivå? Har man tilstrekkelig kunnskap om andre sektorers oppgaver og funksjoner med tilhørende informasjonsbehov? Er terskelen for deling for høy? Finland, som har tilsvarende sektorprinsipp som Norge, anser sektorene som siloer med store glassvinduer som legger til rette for tverrsektorielt samarbeid og informasjonsutveksling.

4.3.1.4 Delingskultur og tillit mellom avsender og mottaker

En forutsetning for god informasjonsdeling er en god delingskultur. Sammensatte trusler krever deling på tvers av etablerte varslings- og rapporteringslinjer i sektorene. Å oppnå en bedre delingskultur krever tillit mellom avsender og mottaker, blant annet til at informasjonens konfidensialitet og integritet ivaretas. Gjensidig tillit bygges gjennom økt forståelse for hverandres prosesser, rutiner, behov og egenart. Dette kan utvikles blant annet gjennom

utdanning og felles trening og øving. Generell kunnskap om hverandre, både faglig og personlig, og erfaring med at sensitiv informasjon ikke lekker er viktig for både offentlig og privat sektor.

4.3.2 Indikatorbasert innhenting (kjente-ukjente)

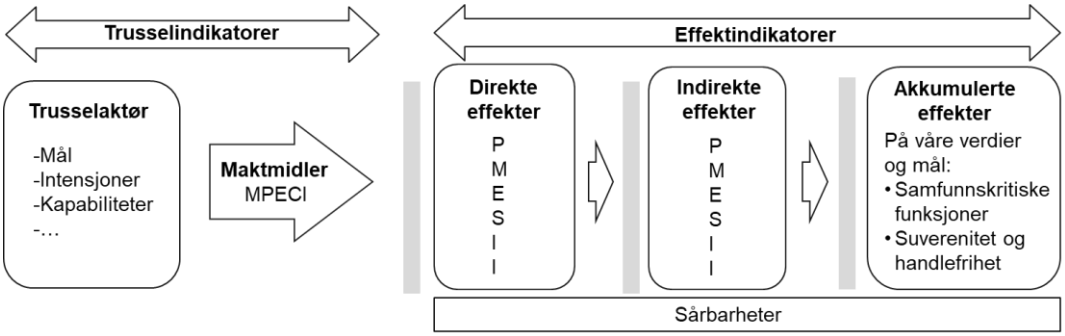
En vanlig måte å samle informasjon på er å benytte indikatorer. En indikator er en variabel som ikke måles direkte, men som sier oss noe om status/tilstand innen et område basert på innsamlet informasjon. For eksempel kan man tenke seg å bruke indikatorer til å monitorere tilstanden på samfunnskritiske funksjoner som tilgjengelighet på kraftforsyning, ekom-tjenester og betalingstjenester.

Evnen til å oppdage trusler, uønskede hendelser og effekter er avhengig av treffsikre indikatorer og at settet med indikatorer er tilstrekkelig korrekt og komplett. Bruk av indikatorer er vanlig i mange sammenhenger for å detektere hendelser som kan gi grunnlag for varsling og rapportering. For at indikatorene skal være relevante med hensyn til å avdekke sammensatte trusler, må de evne å fange opp både trusler og effekter i samfunnet på tvers av samfunnssektorene. I MCDC (Monaghan mfl., 2019) understrekes det at for å understøtte situasjonsforståelse i møte med sammensatte trusler må man utvide indikatorsettet til å omfatte hele MPECI (trusler) og PMESII (effekter). I det videre skiller vi mellom trusselindikatorer og effektindikatorer.

Risiko- og sårbarhetsanalyser (ROS) er som tidligere nevnt en mulig fremgangsmåte for å utlede indikatorer. En ROS-analyse gir svar på spørsmål som: Hva kan gå galt? Hvor sannsynlig er det? Hva er mulige konsekvenser? I analysen beskrives først hvilke mål, verdier og systemer som analysen skal omfatte. Deretter gjøres vurderinger av trusler, sårbarheter og konsekvenser. Samlet danner dette et godt utgangspunkt for å utarbeide relevante trussel- og effektindikatorer.

I Bruvoll et al. (2020) foreslås en fremgangsmåte for å vurdere status og tilstand for kritiske samfunnsfunksjoner.

Figur 4.2 viser sammenhengen mellom trusler (maktmidler relatert til MPECI) og ulike effekter disse kan ha på samfunnet gjennom PMESII-domenene.



Figur 4.2 Sammenheng mellom trussel og effekter.

Figur 4.2 viser hvordan en trusselaktør kan benytte ulike maktmidler for å nå egne mål og intensjoner ved å angripe sårbarheter i de forskjellige PMESII-domenene. Angrepet har en direkte effekt på et mål, men kan også påvirke andre PMESII-domener mer indirekte gjennom avhengigheter. Den samlede/akkumulerte effekten av flere trusler og effekter kan videre påvirke overordnede verdier og målsettinger, som for eksempel vår suverenitet og handlefrihet.

I sammenheng med sammensatte trusler er det behov for å utlede indikatorer som dekker både direkte og indirekte effekter, samt akkumulerte effekter på høyere nivå som kan ha sikkerhetspolitiske implikasjoner. Indikatorene relateres til sårbarheter og verdier vi ønsker beskytte, som for eksempel suverenitet, politisk handlefrihet og Forsvarets operative evne. Ansvar for utvikling og innhenting på effektindikatorene involverer alle samfunnssektorene, inkludert totalforsvaret og private aktører. DSB har et spesielt ansvar med hensyn til informasjonsdeling rundt samfunnskritiske funksjoner og infrastruktur (se samordningskanal kapittel 3). Det er hensiktsmessig å bygge videre på indikatorer, informasjon og ROS-analyser som allerede finnes i sektorene.

Trusselindikatorene skal fange opp trusselhendelser og si noe om egenskaper ved potensielle trusselaktører, som deres strategiske mål, intensjoner og kapabiliteter. Utledning av trusselindikatorer bør støttes av blant annet aktøranalyser, ROS-analyser og scenarioanalyser. Aktøranalyser og innsamling av informasjon på trusselindikatorer tilligger normalt aktører som Etterretningstjenesten, PST og NSM.

Hensikten med begge typer indikatorer er å oppdage avvik fra normaltilstanden. Noen indikatorer er mer generelle, mens andre igjen kan være mer spesifikke med hensyn til trusler og effekter.

I de senere årene har utviklingen gått i retning av at aktører innenfor samfunnssikkerhet og statssikkerhet i økende grad er avhengig av private leverandører av varer og tjenester. Disse avhengighetene introduserer sårbarheter som kan utnyttes av en trusselaktør. Private aktører driver kommersielt og er ikke nødvendigvis alltid like opptatt av sikkerhet, noe som kan gjøre dem mer sårbare ovenfor ulike trusler. Det er derfor viktig at ROS-analysene også omfatter private aktører med roller innenfor samfunns- og statssikkerhet, noe som er i tråd med sikkerhetsloven.

Som beskrevet i kapittel 2 kan sammensatte trusler bestå av både lovlige og ulovlige virkemidler. Lovlige metoder og virkemidler som for eksempel oppkjøp av eiendom og bedrifter, og bruk av ulike former for strategisk kommunikasjon kan kombineres med ulovlige, og eventuelt mer voldelige metoder. Et relevant sett med indikatorer for å oppdage sammensatte trusler må derfor også dekke lovlige metoder og virkemidler. Indikatorene må kunne bidra til å avdekke forsøk på påvirkning av strategiske beslutningsprosesser.[23]

[23] Se for eksempel: Kveberg, Torbjørn, Vårin Alme og Sverre Diesen, *Defence against foreign influence – a value-based approach to define and assess harm, and to direct defence meassures*, FFI-rapport 19/01766.

Indikatorene må også dekke daglig, kontinuerlig påvirkning i et mer langsiktig perspektiv og oppdukkende hendelser. Eksempelvis medieoppslag og bruk av sosiale medier til å spre desinformasjon eller falske nyheter kan påvirke befolkningsgrupper over tid.

Evne til å oppdage sammensatte trusler henger nøye sammen med å ha et godt og relevant indikatorsett, og at informasjon om trusler og effekter deles mellom aktører som har rolle, ansvar og myndighet med hensyn til å oppdage, forebygge og håndtere. Et relevant indikatorsett krever at noen har ansvaret for å oppdatere og vedlikeholde indikatorer over tid.

4.3.3 Oppdage nye, ukjente trusler (ukjente-ukjente)

En anbefaling fra MCDC er at man ikke utelukkende bør satse på indikatorbasert innhenting (Monaghan mfl., 2019). Det bør også brukes metoder utviklet for å oppdage ukjente trusler og effekter, da man antar at det ikke er praktisk mulig å utarbeide og måle på et tilstrekkelig komplett sett med indikatorer. Egenskaper ved sammensatte/hybride trusler åpner for at uventede hendelser kan skje. Dette er trusler og hendelser som man ikke har tenkt på fra før og som vi derfor ikke har indikatorer for. Vi refererer til disse hendelsene som ukjente-ukjente (total ignoranse). For å oppdage denne type avvik fra normalsituasjonen, og sette disse i sammenheng med andre trusler og effekter, må det tilrettelegges for oppdatering av indikator-lister med hjelp av eksempelvis idemyldring, scenarioanalyser og erfaringer. I tillegg kan det være nyttig å ta i bruk metoder og verktøy innen kunstig intelligens og maskinlæring for innsamling og analyse av store datamengder/-strømmer. Dette kan øke evnen til å oppdage anomaliteter og avdekke ukjente mønstre og sammenhenger.

4.4 Analysere og sammenstille informasjon

Analyse og sammenstilling av informasjon er en prosess som har som formål å bygge et relevant tverrsektorielt situasjonsbilde og etablere et hensiktsmessig beslutningsgrunnlag. Et viktig mål er å kunne gjenkjenne sammensatte trusler. Analytikere vil spille en sentral rolle i denne prosessen, og de må ha evne til å analysere situasjonen på tvers av sektorer og nivåer i samfunnet for å utvikle nødvendig situasjonsforståelse.

En stor utfordring med sammensatte trusler er å oppdage og forstå at man faktisk er utsatt for en kampanje og ikke bare mer eller mindre uavhengige enkelthendelser. I utgangspunktet vil uønskede hendelser håndteres i henhold til krisehåndteringsprinsippene om *ansvar, likhet, nærhet* og *samvirke* på lavest mulig nivå innen berørte sektorer. I så måte kan krisehåndterings-prinsippene i seg selv bli en sårbarhet i møte med sammensatte trusler, fordi man på lavere nivå ikke ser at «sin» krise er en del av en større helhet.

Utfordringen er å forstå den akkumulerte (samlede) effekten over tid av flere mindre alvorlige hendelser på eksempelvis vår suverenitet og handlefrihet, og sette dette inn i en sikkerhets-politisk kontekst med kunnskap om mulige trusselaktørers strategiske mål og evner. Dette

understreker viktigheten av å forstå mulige trusselaktører (aktøranalyse)[24], men også egne verdier og sårbarheter (ROS-analyse). Den samlede effekten av trusler og effekter på lavere nivå kan påvirke beslutningsprosesser på høyere nivå. Faren ved å ikke gjenkjenne en kampanje hvor effekter/konsekvenser bygger seg opp over tid, er at man risikerer å behandle symptomene enkeltvis, uten å kurere den «bakenforliggende sykdommen». Sammensatte trusler stiller spesielle krav til analysekapasitet med tverrsektoriell kompetanse, og evne til å følge trusler og effekter over tid og sette disse i sammenheng med sikkerhetspolitisk kontekst. En forutsetning for å kunne oppdage og forstå at man er utsatt for sammensatte trusler er en god forståelse av hva som er normalt – normalsituasjonen. Små endringer over tid vil kunne endre vår oppfatting av hva som er normalt, altså gi en glidning av normalsituasjonen («*boiling frog*»). Akkurat dette kan være spesielt utfordrende å oppdage og forstå, og fordrer at man mer eller mindre kontinuerlig følger med på situasjonen og monitorerer indikatorene.

Et kjennetegn ved sammensatte/hybride trusler er at det benyttes både åpne og fordekte virkemidler. Evne til å attribuere fordekte angrep er en viktig del av analyseprosessen. I dette ligger det å samle konkrete bevis for hvem som står bak.

En hypotesedrevet analyseprosess kan være en hensiktsmessig fremgangsmåte ved mistanke om sammensatte trusler, se for eksempel Heuer (1999) sin metode: *Analysis of competing hypothesis* (ACH). Observasjoner av avvik fra normaltilstanden kan gi mistanke om at det er en sammenheng mellom hendelser. På bakgrunn av dette utarbeides alternative hypoteser, som videre testes mot informasjon som samles inn. Informasjonsinnsamlingen kan her gjøres mer spesifikk ved at man vurderer hvilke indikatorer som har størst forklaringskraft med hensyn til å kunne bekrefte eller avkrefte hypotesene (identifisere drivere). En kjent fare ved en hypotese-drevet prosess er at man i for stor grad fokuserer på å bekrefte hypotesen. I forbindelse med sammensatte trusler er dette muligens ekstra utfordrende fordi det kan være stor usikkerhet og tvetydighet rundt trusler og uønskede hendelser, og sammenhengen mellom disse. Man bør derfor bevisst søke etter informasjon som avkrefter hypotesen, se Heuer (1999).

4.5 Sentral analysekapasitet

MCDC (Monaghan mfl., 2019) understreker at analyse av sammensatte trusler bør være en helhetlig og tverrsektoriell prosess. Det er derfor behov for en sentral analysekapasitet som kan gjennomføre en analyseprosess som beskrevet i kapittel 4.4, og som i det daglige monitorerer og analyserer informasjon for å avdekke sammensatte trusler, og bygge og vedlikeholde et relevant tverrsektorielt situasjonsbilde. En viktig oppgave for analysekapasiteten er å produsere et beslutningsgrunnlag og gi råd til beslutningstakere på sentralt myndighetsnivå. I Støtte og samarbeid (FD/JD, 2018) fremheves nettopp behovet for overordnet koordinering på sentralt myndighetsnivå for å forebygge, oppdage og håndtere sammensatte trusler.

[24] NATO SAS-127 (2017b) poengteres viktigheten av å forstå motstander og hans strategiske mål.

Behovet for en strategisk analysekapasitet er i tråd med anbefalingene fra MCDC (Monaghan mfl., 2019), NATO Stratcom Centre of Exellence (CoE)[25] (Stratcom CoE, 2019) og SAS-127 (NATO, 2017b).

En slik analysekapasitet bør ha et permanent tverrfaglig analysemiljø med kunnskap om potensielle trusselaktører, sårbarheter innen ulike samfunnssektorer og om hvordan trusler kan utnytte sårbarheter som får konsekvenser for stats- og samfunnssikkerhet. Analysegruppen bør understøttes av et nettverk med eksperter innen ulike sektorer og fagområder og akademia. En slik analysekapasitet bør etableres på strategisk nivå (tverrsektorielt nivå) med utgangspunkt i dagens organisasjon. Eksempelvis har Finland etablert et senter i tilknytning til statsministerens kontor (Ferm mfl., 2018) og et nettverk av forskere fra akademia og andre steder for å utvikle beslutningsgrunnlag. I Norge har vi krisestøtteenheten (KSE) med tilhørende situasjonssenter. Det vil være behov for å se rolle, ansvar og myndighet til et slikt senter i lys av krisehåndteringsprinsippene og behovet for tverrsektoriell analyse.

For at analysekapasiteten skal kunne etablere et tverrsektorielt situasjonsbilde og et relevant beslutningsgrunnlag, må den ha tilgang til relevant informasjon om trusler (MPECI/DIMEFIL) og effekter (PMESII) som rammer alle deler av samfunnet (kapittel 4.3). Etablerte informasjonskanaler bør utnyttes og eventuelt styrkes, men det kan også være behov for å etablere nye kanaler.

Det finnes i dag flere situasjonssentre innenfor de ulike sektorene som bygger og vedlikeholder egne situasjonsbilder tilpasset deres behov. Disse sentrene har fagekspertise og informasjon om blant annet samfunnskritiske funksjoner som det kan være relevant å benytte i en tverrsektoriell analyse.

4.6 Internasjonalt samarbeid

I dette konseptgrunnlaget har vi primært tenkt nasjonalt, men fordi sammensatte trusler er et internasjonalt problem, vil det være nødvendig å skape samarbeidsarenaer over landegrensene. Behovet for, og verdien av, internasjonalt samarbeid er fremhevet i MCDC (Monaghan mfl., 2019). Her understrekes det nettopp at utfordringer relatert til sammensatte trusler ikke utelukkende kan løses nasjonalt.

Vi kan for enkelhets skyld dele inn samarbeidet i to typer: Internasjonalt akademisk samarbeid, slik som MCDC og Norges medlemskap i Hybrid COE[26], og operativt samarbeid som etterretningssamarbeid mellom ulike lands EOS-tjenester og politisamarbeid som EUROPOL. Slike samarbeid bidrar med informasjonsutveksling rundt trusler og erfaringer med forebygging og håndtering av sammensatte trusler. På denne måten kan internasjonalt samarbeid bidra til å

[25] NATO Stratcom CoE: « … *an integrated approach across government is needed to efficiently identify and address such threats*…".

[26] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) viktigste oppgave er å være en internasjonal hub for praktikere og eksperter for å bygge/styrke medlemslandenes kapabiliteter og styrke EU-NATO samarbeidet med hensyn til å motvirke hybride trusler: https://www.hybridcoe.fi.

styrke evnen til å oppdage, forebygge og håndtere sammensatte trusler gjennom utveksling av informasjon, analyser og erfaringer på tvers av landegrensene.

Internasjonalt samarbeid kan være enda mer krevende enn tverrsektorielt samarbeid, på grunn av ulikt lovverk, ulike roller og ansvar hos «liknende» organer og sist, men ikke minst, ulike kulturer og språkbarrierer. Imidlertid kan mange av tankene i denne rapporten også benyttes som hjelp i utvikling av en internasjonal situasjonsforståelse.

5 Kunnskap og kompetanse

I kapittel 4 ble det presentert forslag til hvordan man kan bedre evnen til å oppnå situasjonsforståelse i møte med sammensatte trusler. Økt kunnskap og kompetanse er en forutsetning for å få til dette. Sammensatte trusler krever en tverrsektoriell tilnærming hvor det er spesielt viktig å bygge kunnskap og kompetanse rundt tverrsektoriell forhold og problemstillinger. I St. meld. 10 (2016) poengteres det at *«Godt samvirke forutsetter forståelse, tillit og kjennskap til hverandres ressurser, kompetanse, organisering og kultur…».*

Situasjonsforståelse er i henhold til Endsley (1995) avhengig av en rekke individuelle faktorer, som evner, erfaring og egne målsettinger og forventninger. Utdanning, arbeidserfaring, trening og øving bidrar til å utvikle kunnskap, kompetanse og individuelle ferdigheter.

MCDC anbefaler å gjennomføre utdanning, trening og øving av personell og «institusjonelt maskineri» på regulær basis for å styrke evne til å oppdage og håndtere sammensatte trusler.

5.1 Kunnskaps- og kompetansebehov

Basert på innholdet i kapittel 4, vil vi her belyse viktige kunnskaps- og kompetansebehov for å bedre evnen til å oppnå situasjonsforståelsen ved sammensatte trusler. Behovene relateres til sentrale aktiviteter/funksjoner som informasjonsdeling, etablere situasjonsbilde og beslutnings-grunnlag og formidling.

De viktigste rollene nevnt i kapittel 4 er informasjonskilder, analytikere og beslutningstakere. Disse har forskjellige kunnskaps- og kompetansebehov.

5.1.1 Informasjonsdeling

Informasjonsdeling skjer etter push- og pullprinsippene som beskrevet i kapittel 4. Ved varsling og rapportering (push) sendes informasjon fra avsender til én eller flere mottakere. For at relevant informasjon skal nå riktig mottaker til riktig tid, må avsender kjenne til mottakeres informasjonsbehov. Informasjonsbehovet ved sammensatte trusler er sannsynligvis utvidet

sammenliknet med ved normal krisehåndtering når det gjelder informasjon om trusler, sårbarheter og effekter som rammer på tvers av sektorer.

En mottaker, for eksempel en analytiker, kan også etterspørre informasjon (pull) for å dekke egne informasjonsbehov. Dette krever kunnskap om egne informasjonsbehov og om hvor denne informasjonen kan finnes.

Sammensatte trusler som rammer ulike sektorer og nivåer i samfunnet gjør informasjonsdeling ekstra utfordrende. Trusler og hendelser som rammer tverrsektorielt og som påvirker samfunns- og statssikkerheten, må involvere beslutningstakere på strategisk nivå. For å sikre god informasjonsflyt til strategisk nivå bør man styrke kunnskapen om informasjonsbehovet til beslutningstakere på dette nivået. Herunder også kompetansen på lavere nivå om sammensatte trusler, og hvordan disse kan påvirke samfunns- og statssikkerheten.

For å styrke kultur for deling av informasjon og bygge gjensidig tillit er det viktig med kunnskap om andre samfunnssektorer, og deres oppgaver, funksjoner og informasjonsbehov.

Muligheten til å dele informasjon reguleres av forskjellige lover. Det er derfor behov for god kjennskap til lov- og hjemmelsgrunnlaget som gjelder for innsamling og deling av informasjon. Hva har man lov til å samle inn av informasjon, hva har man lov til å dele, og er det mangler i lovverket som hindrer effektiv informasjonsutveksling rundt sammensatte trusler?

Det finnes etablerte mekanismer for informasjonsdeling på tvers av sektorer og nivåer, blant annet samordningskanalen som driftes av DSB (se kapittel 3). Innenfor rammene av totalforsvaret er det etablert flere fora for informasjonsutveksling mellom aktørene. Kunnskap om hvilke muligheter disse mekanismene gir for deling av informasjon er et viktig utgangspunkt for videre arbeid med å bedre informasjonsflyten rundt sammensatte trusler.

5.1.2 Situasjonsbilde og beslutningsgrunnlag

I kapittel 4 beskrives evnen til oppdage og gjenkjenne sammensatte trusler som spesielt utfordrende. Kunnskap om trusler, sårbarheter og mulige effekter er grunnleggende for å utvikle denne evnen. Kunnskap om potensielle trusselaktører og deres mulige strategiske målsettinger, intensjoner og evner er sentralt for å kunne sette trusselhendelser inn i en kontekst som blant annet omfatter den sikkerhetspolitiske situasjonen, ulike narrativ, kapabiliteter og bruk av ulike metoder og virkemidler. Det er også behov for kunnskap om egne sårbarheter, hvordan disse kan rammes/utnyttes, og hvilke direkte og indirekte effekter dette kan ha på samfunnet. Videre må man kunne sette enkelthendelser i sammenheng for å forstå hvordan ulike trusler, som rammer forskjellige sektorer og nivåer, samlet kan påvirke samfunns- og statssikkerheten. Dette stiller krav til kunnskap og kompetanse innen flere områder; forståelse for hvordan samfunnet og krisehåndtering er organisert, hvilke verdier vi ønsker å beskytte og en tverrsektoriell forståelse av risikoer og sårbarheter. God kunnskap om normaltilstanden er en forutsetning for å kunne oppdage og gjenkjenne sammensatte trusler.

Analytikere bør kunne lene seg på et nettverk av eksperter innenfor ulike fagområder og akademia.

Analytikerne bør ha god kunnskap og kompetanse rundt bruk av ulike analysemetoder og verktøy. Bruk av anerkjente metoder og modeller vil kunne bidra til sporbarhet og bedre usikkerhetshåndtering. Dette bidrar videre til å skape tillit og troverdighet til situasjonsbilde og beslutningsgrunnlag.

5.1.3 Formidling og presentasjon

Beslutningsgrunnlag med situasjonsbilde skal bidra til beslutningstakernes situasjonsforståelse. Grunnlaget må derfor svare på deres informasjonsbehov og fremstilles på en måte som understøtter situasjonsforståelse.

5.2 Utdanning

I tråd med anbefalingene fra MCDC CHW, bør et konsept for å styrke situasjonsforståelsen i møte med sammensatte trusler ta utgangspunkt i eksisterende og kjente forhold knyttet til utdanning, trening og øvelser.

Utdanning innenfor ulike fagområder er viktig for å øke kunnskapsnivået rundt sammensatte trusler og hvordan disse kan påvirke oss – både som enkeltindivider og samfunnet. I prinsippet involverer dette alt fra å lære om kildekritikk til mer dyptgående kunnskap innen tema relatert til samfunns- og statssikkerhet. I dette ligger det blant annet å ha kunnskap innen ulike samfunnssektorer, om samfunnskritiske funksjoner og relevante deler av privat sektor. Men kanskje viktigst er tverrsektoriell kunnskap, det vil si kunnskap om hvordan sårbarheter og uønskede hendelser i egen og andres sektorer kan påvirke hverandre, og hvordan dette videre kan få konsekvenser for samfunns- og statssikkerheten. Dette krever blant annet forståelse for hvordan et fritt, liberalt vestlig samfunn virker som system, hvilke deler av dette systemet som det er viktig å forsvare og hvordan dette kan angripes gjennom å utnytte sårbarheter.

Det er behov for utdanning som gir kunnskap om relevante analysemetoder og -teknikker for å kunne analysere og sammenstille informasjon til et situasjonsbilde og beslutningsgrunnlag.

Liaison- og hospitantordninger gir mulighet til å jobbe og skaffe seg erfaring innen andre sektorer. Ordningene bidrar til å øke forståelsen for andre sektorers egenart og behov. Slike ordninger for utveksling av ansatte finnes allerede innenfor flere områder, men det synes å være et potensial for å kunne utnytte dette enda bedre, spesielt med hensyn til sammensatte trusler. Ordninger som dette bidrar til å utvikle nettverk og bygge tillit og kjennskap på tvers sektorer.

5.3 Trening og øving

Trening kan forstås som systematisk og gjentagende repetisjoner, fokusert på konkrete prosedyrer og arbeidsoppgaver, for å utvikle, forbedre eller opprettholde ferdigheter, evner og egenskaper. Individuelle ferdigheter relatert til prosesser, metoder og verktøy er sentralt for effektiv informasjonsinnsamling og billedbygging og bør utvikles gjennom trening.

Virksomheter, deres prosesser og arbeidsoppgaver utvikles ofte gjennom trening og øving. I forbindelse med å oppdage, forebygge og håndtere sammensatte trusler, settes individuelle ferdigheter sammen i et system som har behov for å trenes og øves. Behovet for og verdien av fellesøvelser vil kunne være stort. Det har liten verdi å gjennomføre omfattende øvelser med en dårlig trent organisasjon. Først når kunnskap, erfaring og ferdigheter er etablert til de enkelte elementer (teknikker, verktøy, prosedyrer og arbeidsoppgaver), kan man vurdere å øve systemet som helhet.

Øvelser kan bidra til å øke forståelsen for egen og andres roller i forbindelse med å oppdage og håndtere sammensatte trusler. For eksempel vil en øvelse med et scenario med sammensatte trusler kunne bidra til avklare roller, ansvar og myndighet for forebygging og håndtering, øve opp ferdigheter som evne til å gjenkjenne sammensatte trusler, vurdere risiko og behov for informasjonsdeling og beslutningstaking.

6 Teknologi og infrastruktur

Evnen til å understøtte situasjonsforståelse påvirkes av oppgave- og systemfaktorer som systemdesign, brukergrensesnitt og grad av automatisering (Endsley, 1995). Disse faktorene er nært knyttet opp til bruk av teknologi, og påvirker informasjonsdeling, bildeoppbygging og formidling av bilde og beslutningsgrunnlag. Det er ikke innenfor denne rapportens rammer å gi oversikt over det teknologiske mulighetsrommet, men heller trekke frem noen muligheter som bør vurderes i utviklingen av et konsept for å understøtte situasjonsforståelse i møte med sammensatte trusler.

Informasjons- og kommunikasjonssystemer (IKT) spiller en sentral rolle for evnen til å dele informasjon. Det finnes en mengde ulike systemer, militære og sivile, som støtter informasjonsdeling, men det er ofte problematisk å utveksle informasjon på tvers av systemgrenser på grunn av ulike tekniske løsninger, og ikke minst forskjellige krav til konfidensialitet og integritet. En indikatorbasert innhentingsmetode, som beskrevet i kapittel 4, krever at ulike aktører innen samfunnssektorene, kommunene, fylkene og det private har teknisk mulighet til å formidle informasjon til en analysekapasitet, samtidig som de ivaretar krav til sikkerhet, konfidensialitet, integritet og tilgjengelighet.

Innenfor informasjonsinnsamling, analyse og bildeoppbygging har man behov for å komplettere indikatorbasert innhenting med metoder for å kunne oppdage/avdekke ukjente trusler. Dette er metoder som kan samle inn og analysere store datamengder for å avdekke hendelsesmønstre som avviker fra det som er normalt. Kunstig intelligens, maskinlæring og stordata ble i kapittel 4 nevnt som teknologiområder som kan bidra til å klassifisere og tolke store mengder informasjon og støtte deteksjon av anomaliteter og nye ukjente trusler og handlingsmønstre (oppdage ukjente-ukjente).

IKT-systemer har også en sentral rolle med hensyn til å støtte analyse av situasjonen og i produksjonen av et relevant beslutningsgrunnlag. Et beslutningsstøtteverktøy vil kunne støtte utvikling av handlemåter, vurdering av risiko med mer. Innenfor samfunnssikkerhetsområdet benyttes i dag krisehåndteringssystemet DSB-CIM (se kapittel 3).

Tilgjengelighet på felles og/eller interoperable IKT-systemer er en forutsetning for effektiv informasjonsdeling og bildeoppbygging. Disse systemene bør også ha brukergrensesnitt som tilrettelegger for formidling og presentasjon av situasjonsbilde og beslutningsgrunnlag, for eksempel i form av ulike dashbord.

MCDC anbefaler å utnytte eksisterende infrastruktur i så stor grad som mulig, men denne må tilpasses behovene for bildeoppbygging og analysekapasitet. Det kan i tillegg være behov for å etablere nye fasiliteter og infrastruktur. Dette bør vurderes når nye prosesser for etablering og vedlikeholdelse av situasjonsforståelse utvikles. En helhetlig tilnærming er en forutsetning for å lykkes.

7 Avslutning og anbefalinger

God situasjonsforståelse er en forutsetning for å kunne ta gode beslutninger, men den utfordres i møte med sammensatte trusler. Hensikten med dette konseptgrunnlaget er å støtte utviklingen av én eller flere konseptuelle løsninger for å bedre situasjonsforståelsen rundt sammensatte trusler. I dette kapitlet kommer vi med anbefalinger som er basert på innholdet i grunnlaget.

Vi bruker begrepsforståelsen fra MCDC CHW-prosjektene (Cullen & Reichborn-Kjennerud, 2017): Sammensatte trusler er «*synkronisert bruk av ulike maktmidler for å ramme spesifikke sårbarheter over spektrumet av samfunnsfunksjoner for å oppnå synergistiske effekter*». Maktmidlene kan være av både militær, politisk/diplomatisk, økonomisk, sivil, informasjons-messig, finansiell, etterretningsmessig og juridisk art.

Et konsept for å bedre situasjonsforståelsen rundt sammensatte trusler må hvile på samarbeid og koordinering mellom mange aktører, både nasjonalt og internasjonalt. Det å oppdage, forebygge og håndtere sammensatte trusler er en helhetlig prosess som involverer mange aktører innenfor

statsapparatet. Formålet med et slikt konsept må være at nasjonen Norge blir bedre på å oppdage, attribuere og forstå sammensatte trusler som rammer oss, som grunnlag for å ta gode og tidsriktige beslutninger. Så hvordan kan vi styrke evnen til å oppnå situasjonsforståelse i møte med sammensatte trusler?

I det følgende oppsummeres noen sentrale tema som bør adresseres under konseptutviklingen.

7.1 Generelt

MCDC CHW (Monaghan mfl., 2019) kommer med en rekke anbefalinger for hvordan vi kan bedre evnen til å motstå sammensatte trusler. Noen av disse anbefalinger påvirker også evnen til å oppnå situasjonsforståelse:

- Å oppdage, forebygge og håndtere sammensatte trusler er en helhetlig, tverrsektoriell aktivitet.
- Man bør utnytte eksisterende institusjoner, prosesser og organisasjon så langt det lar seg gjøre, og styrke disse for å møte utfordringene forbundet med sammensatte trusler.
- Håndtering av sammensatte trusler krever en multinasjonal tilnærming. I dette ligger det både operativt samarbeid og kunnskapsutveksling.

I arbeidet med konseptet bør man vurdere styrker og svakheter med dagens krisehåndteringssystem med hensyn på å oppdage, forebygge og håndtere sammensatte trusler. Herunder også se nærmere på hva som eventuelt kan gjøres med prosesser, organisasjon og teknologi for å fremme informasjonsflyt og hindre rivalisering og revirtenkning. Dette er viktig for å kunne gjennomføre nødvendige endringer.

Konseptet bør avklare roller, ansvar og myndighet i forbindelse med å oppdage, forebygge og håndtere sammensatte trusler. Herunder også ansvar for oppdatering og videreutvikling av konsept og systemløsninger.

7.2 Tverrsektorielt situasjonsbilde og beslutningsgrunnlag

Konseptet bør bidra til at det etableres et tverrsektorielt situasjonsbilde for å understøtte situasjonsforståelse i møte med sammensatte trusler. Situasjonsbildet er en del av beslutningsgrunnlaget som presenteres for beslutningstakere.

I arbeidet med konseptet bør det gjøres en vurdering av hva et beslutningsgrunnlag bør inneholde og hvordan dette kan presenteres for ulike beslutningstakere. Her vil det være grunnleggende å avklare hvem som er beslutningstakere og hva som er deres informasjonsbehov. Beslutningsgrunnlaget kan for eksempel bygges opp av ulike «dashbord» som gir oversikt over trusler, uønskede hendelser og effekter som samlet/akkumulert kan påvirke samfunns- og

statssikkerheten. Videre bør det inneholde informasjon fra aktøranalyser, risiko- og sårbarhetsvurderinger og analyse av hypoteser relatert til om vi er utsatt for sammensatte trusler eller ikke.

7.3 Strategisk analysekapasitet

Konseptet bør bidra til at det etableres en strategisk analysekapasitet for tverrsektorielle analyser av sammensatte trusler. Denne bør ha som sine viktigste oppgaver å monitorere situasjonen, oppdage og attribuere trusler, bygge et tverrsektorielt situasjonsbilde og utarbeide et relevant beslutningsgrunnlag.

Analysekapasiteten bør etableres på strategisk nivå og ha en permanent bemanning som kan støtte seg på et nettverk av fageksperter og akademia.

7.4 Analyseprosess

Konseptet bør bidra til at det utvikles en analyseprosess som er egnet for å bygge og vedlikeholde et tverrsektorielt situasjonsbilde og utarbeide beslutningsgrunnlag. Analyseprosessen krever god kjennskap til normaltilstanden i samfunnet rundt trusler og effekter for å kunne oppdage avvik/anomaliteter.

7.5 Informasjonsdeling

Konseptet bør bidra til å styrke evne og vilje til å dele informasjon på tvers av sektorer, nivåer og aktører for å understøtte situasjonsforståelse rundt sammensatte trusler. I dette ligger det å utvikle og beskrive informasjonsbehovene til ulike aktører med roller, ansvar og myndighet knyttet til å oppdage, forbygge og håndtere sammensatte trusler.

Konseptet bør legge til rette for å kunne utnytte både push- og pullprinsippet for deling av informasjon.

Konseptet bør bidra til å etablere informasjonskanaler som dekker alle relevante informasjonskilder innen statlig- og kommunal sektor samt private aktører med roller innenfor samfunns- og statssikkerhet.

Konseptet bør bidra til å videreutvikle og styrke delingskulturen for informasjon, og tilrettelegge for samarbeid og koordinering. Dette innebærer også å vurdere styrker og svakheter ved dagens krisehåndteringssystem med hensyn til deling av informasjon i møte med sammensatte trusler.

I arbeidet med konseptet bør man vurdere ulike tiltak for å bygge tillit mellom aktører og organisasjoner, slik at frykten reduseres for at informasjon skal komme på avveie eller misbrukes. Felles trening, øving og utdanning sammen med liaison- og hospitantordninger, støtter dette og bidrar til respekt for andres kompetanse og innsikt i hverandres utfordringer og

perspektiver. Dette bidrar til kunnskap om andres aktørers oppgaver og funksjoner og innsikt i deres informasjonsbehov.

Informasjonsbehov kan uttrykkes ved bruk av indikatorer knyttet til kjente trusler og sårbarheter (såkalte kjente-ukjente). Indikatorsettet må dekke alle kjente politiske/diplomatiske, militære, økonomiske, informasjonsmessige, etterretningsmessige og legale maktmidler som kan tenkes benyttet mot våre sårbarheter. I tillegg må indikatorene dekke sårbarheter og effekter som kan påvirke politisk, militært, økonomisk, sosialt, informasjon og infrastruktur. For å ha et oppdatert og relevant indikatorsett, er det er behov for gode, tverrsektorielle rutiner for å oppdatere og komplettere settet med indikatorer.

MCDC CHW anbefaler å komplettere indikatorbasert innhenting med metoder for å oppdage ukjente trusler og sårbarheter (såkalte ukjente-ukjente). Her kan det være aktuelt å benytte metoder og verktøy innen kunstig intelligens, maskinlæring og stordata.

I forbindelse med konseptarbeidet er det behov for å gjøre en vurdering av om lovverk og hjemmelsgrunnlag i tilstrekkelig grad åpner opp for innsamling og deling av informasjon rundt sammensatte trusler. Dette gjelder spesielt lovverk som regulerer innsamling av informasjon rundt lovlig virksomhet.

7.6 Kunnskap og kompetanse

Kunnskap og kompetanse er fundamentet for å styrke evnen til situasjonsforståelse rundt sammensatte trusler. Konseptet bør derfor bidra til å etablere en oversikt over sentrale kunnskaps- og kompetansebehov, og beskrive hvordan dette kan oppnås gjennom blant annet utdanning, trening og øving.

Konseptet bør videre beskrive behovet for å løfte det generelle kunnskapsnivået i samfunnet og innenfor samfunnssektorene rundt sammensatte trusler og påvirkning. Dette kan bidra til å styrke varsling og rapportering rundt mistenkelige aktiviteter og hendelser.

Konseptet bør fremheve viktigheten av (felles) utdanning, trening og øving, og liaison- og hospitantordninger i arbeidet med å forbedre evnen til å oppdage, forebygge og håndtere sammensatte trusler.

7.7 Teknologi

Konseptet bør beskrive ulike teknologiske muligheter for å understøtte bildeoppbygging og situasjonsforståelse rundt sammensatte trusler. Spesielt gjelder dette IKT-systemer som støtter informasjonsdeling og innsamling, analyse, sammenstilling og presentasjon av informasjon. Det er behov for systemer for deling av informasjon på riktig graderingsnivå, som ivaretar konfidensialiteten og integriteten på informasjonen.

Forkortelser

ACH	Analysis of competing hypothesis
ANNCP	Anglo, Netherlands, Norwegian cooperation program
CHW	Countering hybrid warfare
BFF	Beredskapssystem for forsvarssektoren
CoE	Centre of excellence
DIMEFIL	Diplomatic, Informational, Military, Economic, Finance, Intelligence and Law Enforcement (Legal)
DSB	Direktoratet for samfunnssikkerhet og beredskap
EOS	Etterretning og sikkerhet
ETj	Etterretningstjenesten
FD	Forsvarsdepartementet
FOH	Forsvarets operative hovedkvarter
HV	Heimevernet
IKT	Informasjons- og kommunikasjonssystemer
JD	Justisdepartementet
KSE	Krisestøtteenheten
MCDC	Multinational capability development campaign
MPECI	Military, Political, Economic, Civil, Information
NSM	Nasjonal sikkerhetsmyndighet
PMESII	Political, Military, Economic, Social, Informational, Infrastructure
POD	Politidirektoratet
PST	Politiets sikkerhetstjeneste
ROS	Risiko- og sårbarhetsanalyser
SBS	Sivilt beredskapssystem

Referanser

Bruvoll, J. A., Endregard, M. og Busmundrud, O. (2020). Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger. FFI-rapport 20/02355.

Bruvoll, J. A., Endregard, M., Brattekås, K. og Nystuen, K. O. (2018). Sikkerhetspolitisk krisehåndtering på strategisk nivå. FFI-rapport 18/01164. BEGRENSET.

Cullen, P. J., Reichborn-Kjennerud, E. (2017). MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC januar 2017.

Diesen, S. (2018). Lavintensivt hybridangrep på Norge i en fremtidig konflikt. FFI-rapport 18/00080.

DSB (2014). Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen. Direktoratet for samfunnssikkerhet og beredskap (DSB) 2014.

DSB (2017). Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprett-holde til enhver tid? Direktoratet for samfunnssikkerhet og beredskap (DSB) 2017.

DSB (2019). Analyse av krisescenarioer. Direktoratet for samfunnssikkerhet og beredskap (DSB) 2019.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors, 1995, 37(1), 32-64.

Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L., Sellevåg, S. R. og Pham, V. (2020). Utvikling av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet. FFI-rapport 20/01745, Unntatt offentlighet.

Ferm, T. et al. (2018). A description of two national conceptual approaches for establishing Hybrid Threat / Hybrid Influence Situational Awareness. FFI-eksternnotat 18/02098.

Forsvarsdepartementet (FD) (2020). Prop. 14 S (2020-2021): Evne til forsvar – vilje til beredskap.

Forsvarsdepartementet (FD) og Justis- og beredskapsdepartementet (JD) (2018): Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.

Forsvarets høgskole (FHS) (2019). Forsvarets fellesoperative doktrine (FFOD).

Forsvarets operative hovedkvarter (FOH) (2018): Norsk vertslandsstøttekonsept til bruk i totalforsvaret. Utkast til prøve 2018-2020, februar 2018.

Grunnan, T., Endregard, M., Siedler, R. E. og Elstad, A. K. (2020). Norwegian societal security and state security – challenges ad dilemmas. Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Confernce.

Heuer R. J. (1999). Psychology of Intelligence Analysis. Center for the study of intelligence. CIA, 1999.

Justis- og beredskapsdepartementet (JD) (2020). Meld. St. 5 (2020–2021): Samfunnssikkerhet I en usikker verden.

Justis- og beredskapsdepartementet (JD) (2017). Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen). Justis- og beredskapsdepartementet, 1. September 2017.

Malerud, S. og Toverød, N. (2019). Intervju med liaisoner under Trident Juncture 2018. FFI-internnotat 19/02165. BEGRENSET.

Monaghan, S., Cullen, P. og Wegge, N. (2019). MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, MCDC mars 2019.

NATO (2017a). The NATO alternative analysis handbook. Second edition, oktober 2017.

NATO (2017b). SAS-127 Research Specialist Team on Hybrid Warfare: Implications for NATO. STO Techical Report, AC/323. Pre-release.

Pettyjohn, S. L. og Wasser, B. (2019). Competing in the Gray Zone. Russian Tactics and Western Responses. RAND Corporation, Santa Monica, California.

Rausand, M. & Utne, I. B. (2011). Risikoanalyse – teori og metoder. Tapir akademisk forlag, Trodheim.

Stratcom CoE (2019): Hybrid Threats. A Strategic Communications Perspective. NATO Stratcom Centre of Excellence.

Toverød, N., Malerud, S. og Fridheim, H. (2020). Oppsummering AltA aktivitet 27. november 2019. Rammeverk for konsept til støtte for situasjonsforståelse relatert til hybride trusler/påvirkningsoperasjoner. FFI-eksternnotat 20/00094. Unntatt offentlighet.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

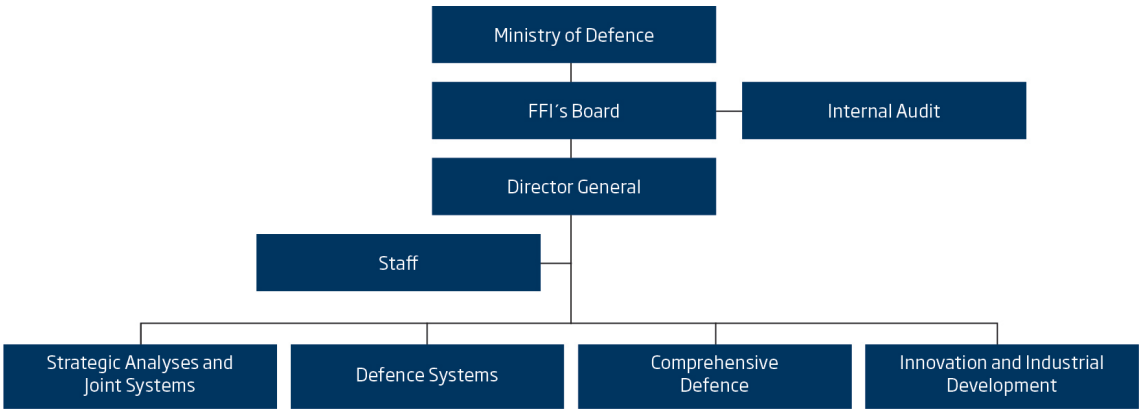
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt