FFI Forsvarets forskningsinstitutt

23/01897

FFI-RAPPORT

# Forsvar mot fremmedstatlige påvirkningsoperasjoner

## – etablering av funksjon i forsvarssektoren

Eskil Grendahl Sivertsen
Paul Buvarp

# Forsvar mot fremmedstatlige påvirkningsoperasjoner
## – etablering av funksjon i forsvarssektoren

Eskil Grendahl Sivertsen
Paul Buvarp

Forsvarets forskningsinstitutt (FFI) 5. april 2024

**Emneord**
Påvirkningsoperasjoner
Kognitiv krigføring
Desinformasjon

**FFI-rapport**
23/01897

**Prosjektnummer**
1692

**Elektronisk ISBN**

978-82-464-3494-0

**Engelsk tittel**
Defence against foreign influence operations – establishing a function in the defence sector

**Godkjennere**

Stig Rune Sellevåg, *forskningsleder*
Janet Blatny, *forskningsdirektør*

*Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur*.

# Sammendrag

Denne rapporten er et kunnskapsgrunnlag bestilt av Forsvarsdepartementet. Den gir vurderinger av hvordan forsvarssektoren kan etablere en egen funksjon for å skape situasjonsforståelse i informasjonsmiljøet og forebygge, avdekke og håndtere utenlandske påvirkningsoperasjoner. I denne rapporten kaller vi denne typen operasjoner for FIMI, fra det engelske *Foreign Information Manipulation and Interference*, eller utenlandsk informasjonsmanipulasjon og innblanding. En funksjon mot dette kaller vi et FIMI-forsvar.

Litteraturstudier viser til en håndfull anbefalinger om mønsterpraksis for en slik funksjon. Studiene peker på at det er viktig å integrere analyse i alle funksjonens prosesser. De poengterer også at åpen og god kommunikasjon er essensielt, både internt i funksjonen og mellom funksjonen og andre etater og interessenter.

Hoveddelen av vurderingene våre bygger på en casestudie av Sveriges *Myndigheten för psykologiskt försvar*. Vi går gjennom bakgrunnen for myndigheten og ansvaret, oppgavene og mandatet dens i tillegg til organiseringen, etatsstyringen og selve utøvelsen av myndighetens virksomhet. Vi går også kort gjennom Litauens nasjonale krisehåndteringssenter og funksjon i det litauiske forsvaret.

Vi beskriver deretter ulike forhold som danner konteksten rundt et FIMI-forsvar i forsvarssektoren. Her diskuterer vi Nato-doktriner, Natos fremtidige konsept for kognitiv krigføring, annen alliert samhandling og internasjonale arenaer. Vi diskuterer også koblingen til Forsvaret og andre relevante, nasjonale virksomheter.

I analysene våre finner vi fem behov et FIMI-forsvar i forsvarssektoren bør dekke: å etablere situasjonsforståelse, å oppdage FIMI-forsøk, å utvikle responsopsjoner, å drive forebygging mot FIMI og å koordinere nasjonal og internasjonal innsats. På bakgrunn av disse behovene har vi utarbeidet en serie med prinsipper som et slikt forsvar *må* og *bør* følge.

Vurderingen går videre med betraktninger om FIMI-forsvarets mulige organisering og struktur og noen etiske og juridiske problemstillinger.

Vi anbefaler at et FIMI-forsvar har ansvar for å etablere situasjonsforståelse i informasjons-miljøet. FIMI-forsvaret må oppdage FIMI-aktivitet, utvikle responsopsjoner til det og forebygge mot det. Personell tilknyttet FIMI-forsvaret bør også ivareta nasjonal og internasjonal deltakelse og kunnskapsdeling i relevante fora.

Vi anbefaler at FIMI-forsvaret bygger analytisk kapasitet som grunnlag i arbeidet og tilegner seg personell med relevant kompetanse. I tillegg må det utarbeides et mandat for FIMI-forsvaret og en egen utredning av digitale verktøy og om et mulig hjemmelsgrunnlag for et slikt forsvar.

Vi anbefaler at et slikt FIMI-forsvar bygges slik at det i fremtiden kan samvirke med en større, tverrsektoriell funksjon.

# Summary

This report considers issues regarding the establishment of a potential function in the defence sector to create situational awareness amongst information professionals and to detect and counter what the EU identifies as *Foreign Information Manipulation and Interference*, or FIMI.

Literature reviews show a handful of recommendations for best practices that such a function should follow. They point out that it is important to integrate analysis into all of the function's processes. Furthermore, they point out that transparent and effective communication is essential, both within the function and between the function and other agencies and stakeholders.

The main thrust of our examination is based on a case study of Sweden's Psychological Defence Agency. Our report describes the background for the agency, its responsibilities, tasks, and mandate, as well as organisation, state leadership, and the practice of the agency's activities. We also briefly examine the Lithuanian National Crisis Management Centre and its function in the Lithuanian Armed Forces.

Our report then deals with the context of this kind of function against FIMI in Norway. Our discussion focusses on NATO doctrines, NATO's future concept of cognitive warfare, other allied cooperation, and international arenas. In addition, our discussion covers the relationship to the Norwegian Armed Forces and other relevant national institutions.

In our analysis, we identify five requirements for a Norwegian FIMI defence: to establish situational awareness, to detect attempts at FIMI, to develop responses, to build resilience and preparedness against FIMI, and to develop national and international coordination. Based on these requirements, we have developed a list of principles that such a defence must or should adhere to.

Our report then considers the FIMI defence's possible organisation and structure as well as specific ethical and legal questions.

We recommend that a FIMI defence be responsible for establishing situational awareness amongst information professionals. The FIMI defence must detect FIMI activity and develop response options and preventive measures against FIMI. The FIMI defence should also coordinate national and international participation and knowledge exchange in relevant forums.

We recommend that a FIMI defence builds analytical capacity as a foundation through its activities and gathers personnel with relevant skills. Additionally, a mandate for a FIMI defence must be defined, and assessments of suitable digital tools and a possible legal framework for the defence should be carried out.

We recommend that a FIMI defence be built in such a way that it will be compatible with a larger, multisectoral function in the future.

# Innhold

# Forord

Fremmedstatlige påvirkningsoperasjoner, i denne rapporten kalt *Foreign Information Manipulation and Interference (FIMI)*, kan svekke tilliten i samfunnet, undergrave demokratiske prosesser, motarbeide norske interesser utenlands og svekke politisk og militært handlingsrom i hele krisespekteret.

Å skape forsvarsevne mot FIMI krever en helhetlig situasjonsforståelse i informasjonsmiljøet og en samlet innsats fra hele samfunnet. Samtidig har forsvarssektoren – som andre sektorer – et ansvar for å identifisere egne sårbarheter, vurdere risiko og bygge en evne til å forebygge, avdekke og håndtere slike operasjoner i en sikkerhetspolitisk spent og usikker tid med økt stormaktsrivalisering og kamp om narrativer.

Denne rapporten er skrevet på oppdrag fra Forsvarsdepartementet for å skape et kunnskapsgrunnlag for hvordan en funksjon for FIMI-forsvar for forsvarssektoren kan etableres, basert på mønsterpraksis og inspirasjon fra Sveriges *Myndigheten för psykologiskt försvar (MPF)*. Vi vil rette en stor takk til Sveriges MPF og litauiske myndigheter for å åpent dele informasjon og erfaringer med oss i arbeidet med å skrive denne rapporten, og til kollega Torgeir Mørkved for gode innspill.

Kjeller, 12.06.23

Eskil Grendahl Sivertsen og Paul Buvarp

# 1 Innledning

Forsvarsdepartementet (FD) har gitt FFI i oppdrag å utvikle et kunnskapsgrunnlag for hvordan forsvarssektoren kan etablere en egen funksjon på strategisk nivå for å styrke Norges forsvarsevne mot utenlandsk, utilbørlig påvirkning mot Norge og norske interesser.

I oppdraget bes det spesielt om å se hen til Sveriges *Myndigheten för psykologiskt försvar*, men også andre relevante aktører og mønsterpraksis så langt dette er mulig innenfor en kort tidsfrist. Basert på litteraturgjennomgang av mønsterpraksis og erfaringer fra Sverige og Litauen, beskriver denne rapporten hvordan en slik funksjon kan etableres tilpasset norske forhold og behov, med vekt på forsvarssektorens rolle for å møte utfordringer knyttet til global informasjonskrigføring.

Dette er et felt hvor flere begreper brukes, blant annet påvirkningsoperasjoner, informasjonskrig, kognitiv krigføring og psykologiske operasjoner. Bildet kompliseres av at denne formen for sammensatte trusler ikke lar seg definere som en militær eller sivil utfordring, men rammer samfunnet på tvers av sektorer i hele krisespekteret.

I denne rapporten bruker vi begrepet Foreign Information Manipulation and Interference (FIMI), basert på definisjonen til EUs External Action Service (EEAS) som beskrevet i rapporten *1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*.[1]

> *FIMI is a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory*. (ibid.)

FIMI har blitt et etablert maktpolitisk virkemiddel. Det brukes ofte som en del av sammensatte trusler og er en styrkemultiplikator for disse. Slike operasjoner kan svekke tilliten i samfunnet, undergrave demokratiske prosesser, motarbeide norske interesser utenlands og svekke politisk og militært handlingsrom i hele krisespekteret.

FIMI står høyt på agendaen i Nato, EU og blant allierte. Ifølge Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten (ETJ) er Russland og Kina de to fremmedstatlige aktørene som utgjør den viktigste trusselen mot Norge og norske interesser, samfunnssikkerhet og statssikkerhet.

Å forebygge, detektere og håndtere FIMI forutsetter situasjonsforståelse i informasjonsmiljøet. Dette krever kunnskap, ferdigheter og IKT-verktøy for kartlegging og analyse. Mens andre stater i det transatlantiske og europeiske felleskapet har utviklet kapabiliteter for dette, har

[1] *1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*. (2023). European External Action Service. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

Norge i begrenset grad gjort det samme. I en tidligere FFI-rapport poengteres det at det er «fortsatt uavklart hvem som har det overordnede ansvaret for å forebygge, oppdage, kartlegge, analysere og håndtere påvirkningsaksjoner».[2]

Fordi FIMI er både en militær og en sivil utfordring, og treffer hele samfunnet på tvers av sektorer, er det uklart hvilken rolle Forsvaret og forsvarssektoren skal ha i å forebygge, detektere og håndtere slike trusler i informasjonsmiljøet. Det finnes ikke et «militært» og et «sivilt» informasjonsmiljø. Effekter skapt utenfor forsvarssektorens ansvarsområde kan få konsekvenser for militært handlingsrom. Det betyr at Forsvarsdepartementet og Forsvaret har behov for å etablere situasjonsforståelse i informasjonsmiljøet som ikke er begrenset til egen sektor.

Dette er konklusjoner som også beskrives i Forsvarskommisjonen av 2021. Der beskrives et behov for å utvikle Forsvarets «evne til å forsvare seg mot trusler i informasjonsdomenet».[3] Dette «bør komme på plass så fort som mulig».[4]

## 1.1 Metode

Oppdraget ble løst ved to forskjellige metoder for informasjonsinnhenting: litteraturstudier og semi-strukturerte intervjuer.

For litteraturstudien ble en rekke publikasjoner og databaser undersøkt for å finne relevant informasjon til oppdraget. FFI har, gjennom annet arbeid med FIMI-problemstillinger, fått god kunnskap om og tilgang til forskning på dette feltet. Litteraturstudien viser til mønsterpraksis i et teoretisk perspektiv, og gir et utklipp av faktorer som kan være nyttige å ha med seg i etableringen av en funksjon.

Hovedvekten av vurderingen ligger i intervjuene som ble gjort. FFIs forskere reiste til Sverige og til Litauen for å snakke med egnede aktører der. Selve intervjuene ble gjennomført fysisk og med flere personer. Formatet for intervjuene var såkalte semi-strukturerte intervjuer. Dette innebærer at intervjuerne har en løs plan for tematikken de vil dekke, men gir den intervjuede rom til å svare også utover det intervjueren spør direkte om. Det gir også intervjuerne mulighet til å etterfølge interessante, oppdukkende elementer som kanskje ikke var ventet på forhånd. Dette er en egnet metode for å fange opp informasjon utenfor intervjuernes forutinntatte kunnskap og gir mer mulighet til utforsking og dialog.

[2] Klepper, K. B., et al. (2023) *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv*. FFI-rapport 23/00879. Forsvarets forskningsinstitutt.
[3] NOU 2023:14. (2023). *Forsvarskommisjonen av 2021 — Forsvar for fred og frihet*. regjeringen.no/contentassets/8b8a7fc642f44ef5b27a1465301492ff/no/pdfs/nou202320230014000dddpdfs.pdf. s. 208.
[4] Ibid, s. 207.

# 2 Litteraturstudier av mønsterpraksis

Ettersom flere andre land har etablert funksjoner som kan ligne på en tenkt norsk funksjon finnes det også forskning og rapportering som kan bistå i utformingen. Noe litteratur tar et teoretisk perspektiv på FIMI og beskriver mønsterpraksis på å håndtere disse. Annen litteratur ser på etablerte funksjoner og hvilke lærdommer som er blitt tilegnet i drift av disse. En rask gjennomgang av noe av denne litteraturen kan utmeisle noen konkrete poenger som vil være verdt å ta med seg i den videre analysen. Disse kan enten bekrefte og understøtte funn fra de konkrete analysene som følger, eller tillegge nye elementer til prioritering i en norsk funksjon.

Det skal nevnes at det er lite åpenhet rundt dette temaet generelt, ettersom nasjoner vil verne om egen praksis ovenfor motstandere. Gjennom deltakelse i internasjonale partnerskap kan FFI få tilgang til informasjon som kan være til nytte.

The International Partnership to Counter State-sponsored Disinformation utarbeidet en serie med såkalte prinsipper på et analyseforum i Washington D.C. i januar 2023.[5] Prinsippene, utarbeidet og godkjent i plenum var som følger:

1. Kultiver en lagmentalitet på tvers av hele funksjonen og de ulike rollene
2. Kultiver en lavtersklet kommunikasjonskultur internt i funksjonen
3. Forstå hva som allerede eksisterer og bygg oppå dette
4. Prioriter handlinger og analyse
5. Vær klar på hvem som skal bruke analysen til hvilket formål
6. Tenk på hva som kan deles og unngå gradering der mulig
7. Vær klar over begrensningene med analyse
8. Ha enighet om systemer og formater for deling av analyse
9. Integrer analyse i hvert steg
10. Del videre mønsterpraksis og suksesser

[5] Buvarp, P. M. H. (2023) *International Partnership to Counter Statesponsored Disinformation Meeting Participation, January 2023 ─ Meeting summary with detailed appendices*. FFI-Notat 23/00718. Forsvarets forskningsinstitutt. (U. Off.)

Prinsippene samlet viser viktigheten av åpen kommunikasjon, integrerte arbeidsgrupper og analyse som fundament. Dette kan være gode grunnsteiner å basere en eventuell norsk funksjon på.

Et skriv fra USAs Global Engagement Center, «Academic & Think Tank Highlights» fra 2020/2021[6] peker på en rekke anbefalinger for å kontre desinformasjon. To anbefalinger er verdt å ta med seg i norsk kontekst. De peker blant annet på viktigheten av å jobbe tett sammen med forskning, ved å dele data og gi forskere evnen til å drive dypere analyse, testing og utvikling av verktøy. Det neste de peker på er viktigheten av samarbeid på tvers av sektorer. Dette vil øke tilgjengelige ressurser, gi bedre tilgang til data, og bidra til å standardisere definisjoner og praksiser.

Britiske Institute for Strategic Dialogue har også rapporten «Best Practices in Detecting and Analysing Foreign State Online Manipulation»[7] hvor kapabilitetskrav til deteksjon og analyse av desinformasjon er drøftet. Det er grundig poengtert at disse kapabilitetene skal fungere sammenkoblet med hverandre. Rapporten peker på fire kapabilitetsområder:

1. Analytikere som jobber med store datasett og er tettest på systemet.

2. Teknologiske utviklere og visualiseringsutviklere som modellerer, prosesserer og er kjent med de nyeste teknologiske verktøyene.

3. Fageksperter som har dyp kunnskap om desinformasjonsaktører, desinformasjonsmål, og de temaene som er gjenstand for desinformasjon.

4. OSINT-eksperter som kan undersøke de mest presserende analytiske funnene for å finne detaljer om desinformasjonsaktøren eller nettverket bak.

Samlet sett viser innspillene fra disse kildene at man bør etterstrebe et tett samarbeid mellom ulike kapabiliteter og fag. Analyse, fag og forskning, teknisk utvikling og visualisering står sentralt, men det er viktig å bygge ned skillene mellom disse, og at de integreres på tvers. Det er også anbefalt å koble disse kapabilitetene på tvers av sektorer for å hindre dupliserende arbeid, koordinere forståelse og utnytte ressurser på best mulig måte.

FFI har også tidligere gjennomført komparative studier av andre lands tilnærming til sammensatte trusler, hvorav FIMI er et tilhørende element. Rapporten i sin helhet er relevant for å se til lærdommer fra andre land, men med tanke på FIMI direkte kan det være nyttig å se til analysen om Storbritannia. Der har det blitt etablert et verktøysett som kalles RESIST 2 og består av elementene Recognise, Early Warning, Situational Insight, Impact Analysis, Strategic Communications, og Tracking Effectiveness. Verktøysettet kan brukes av mange forskjellige

[6] *Academic & Think Tank Highlights*. (2021). Global Engagement Center Academic & Think Tank Outreach Unit. (Unclassified).
[7] *Best Practices in Detecting and Analysing Foreign State Online Manipulation*. (2020). The Institute for Strategic Dialogue.

typer aktører og skal «bidra til forståelse for hvordan mis- og desinformasjon kan identifiseres, takles, besvares og motvirkes».[8]

# 3 Case studier: Sverige og Litauen

FD har spesielt bedt om en beskrivelse av Sveriges nyetablerte *Myndigheten för psykologiskt försvar* (MPF) og en vurdering av hvordan en slik type funksjon kan tilpasses norske forhold og behov, med vekt på forsvarssektorens rolle for å møte utfordringer knyttet til FIMI. I tillegg har vi valgt å beskrive hvordan Litauen har gjort det. Mens Sveriges MPF er en egen, sivil etat frikoblet fra etterretningstjenestene og Forsvaret og med et totalansvar for å koordinere og styrke hele Sveriges psykologiske forsvar, har Litauen etablert sine funksjoner i forsvarssektoren. Dette er to ulike tilnærminger som i sum kan gi nyttig kunnskap og erfaringer som, sammen med litteraturgjennomgangen av mønsterpraksis, er relevante for å gi anbefalinger for hvordan en slik funksjon kan etableres i en norsk totalforsvarskontekst, plassert på strategisk nivå i forsvarssektoren.

## 3.1 Sverige: Myndigheten for psykologisk forsvar

### 3.1.1 Bakgrunn

Sveriges psykologiske forsvar ble etablert på 1950-tallet som det fjerde området av totalforsvaret i tillegg til det militære, sivile og økonomiske. Det psykologiske forsvaret var virksomt fram til 1970-tallet, da det ble nedprioritert.

Som en konsekvens av en forverret sikkerhetspolitisk situasjon, ble det psykologiske forsvaret igjen løftet fram i 2014 i Försvarsberedningens rapport *Försvaret av Sverige - Starkare försvar för en osäker tid* (Ds 2014:20).[9] I 2019 iverksatte den svenske regjeringen en utredning i den hensikt å etablere en egen myndighet for å utvikle og samordne Sveriges psykologiske forsvar, og i 2020 kom anbefalingen *En ny myndighet för att stärka det psykologiska försvaret* (SOU 2020:29).[10]

Sveriges *Myndighet för psykologiskt försvar*[11] (MPF) ble etablert 1. januar 2022 som en egen myndighet (etat) underlagt regjeringen gjennom Forsvarsdepartementet. Myndighetens formål

[8] Bergaust, J. C. et al. (2022). *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen.* FFI-rapport 22/02310. Forsvarets forskningsinstitutt.
[9] Ds 2014:20. (2014). *Försvaret av Sverige - Starkare försvar för en osäker tid.* Försvarsberedningen. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2014/05/ds-201420/
[10] SOU 2020:29. (2020). *En ny myndighet för att stärka det psykologiska försvaret.* Statens Offentliga Utredningar. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2020/05/sou-202029/
[11] *Myndigheten för psykologiskt försvar.* Myndigheten för psykologiskt försvar. https://www.mpf.se

er «å verne om det åpne og demokratiske samfunnet, den frie meningsdannelsen og Sveriges frihet og uavhengighet».[12] MPF overtok også det forskningsfaglige ansvaret for psykologisk forsvar, som inntil da hadde ligget på *Myndigheten för samhällsskydd och beredskap* (MSB).[13] MSB kan kan sammenlignes med det norske *Direktoratet for samfunnssikkerhet og beredskap* (DSB).

### 3.1.2 Ansvar og oppgaver

*Myndigheten for psykologisk forsvars* hovedoppgave er å «lede arbeidet med samordning og utvikling av svenske myndigheters og andre aktørers virksomhet innen Sveriges psykologiske forsvar»[14]. Sveriges psykologiske forsvar er imidlertid ikke en oppgave MPF skal ivareta alene, men noe myndighetene, kommunene, organisasjonene og innbyggerne skaper sammen i tråd med totalforsvarets prinsipper og logikk. MPF har det faglige og operative ansvaret for å bygge og drifte et sterkt, nasjonalt psykologisk forsvar. Myndighetens ansvar kan oppsummeres i fire hovedpunkter:

1. Lede arbeidet med å utvikle Sveriges psykologiske forsvar

2. Samordne, koordinere og støtte statlige og ikke-statlige aktører og deres aktiviteter relatert til det psykologiske forsvaret, som et bidrag til et sterkt totalforsvar

3. Styrke befolkningens motstandskraft mot desinformasjon og påvirkningskampanjer

4. Identifisere, analysere, imøtegå og forebygge utilbørlig informasjonspåvirkning og annen villedende informasjon som rettes mot Sverige eller svenske interesser fra utenlandske aktører

### 3.1.3 Mandat

Følgende tekst er oversatt til norsk fra forskriften *Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar.*[15]

§ 1 Myndigheten for psykologisk forsvar skal i fredstid og ved høy beredskap:

- Lede arbeidet med å samordne og utvikle myndighetenes og andre aktørers virksomhet innen Sveriges psykologiske forsvar.

- Gi støtte til slik virksomhet og

[12] *Uppdraget*. Myndigheten för psykologiskt försvar. https://www.mpf.se/vart-uppdrag/
[13] *Myndigheten för samhällsskydd och beredskap*. Myndigheten för samhällsskydd och beredskap. https://www.msb.se/
[14] *Uppdraget.*
[15] Kommittédirektiv 2021:936. (2021). *Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar.* https://riksdagen.se/sv/dokument-lagar/dokument/kommittedirektiv/forordning-2021936-med-instruktion-for_H9B1936

- Bidra til å styrke befolkningens motstandskraft

§ 2 Myndigheten skal spesielt:

1. identifisere, analysere og kunne gi støtte i møtet med utilbørlig informasjonspåvirkning og annen villedende informasjon som rettes mot Sverige eller svenske interesser,

2. spre kunnskap og bidra til befolkningens og berørte aktørers beredskap i spørsmål om psykologisk forsvar,

3. gjennomføre utdanning og øvingsvirksomhet innenfor myndighetens ansvarsområde,

4. følge, bestille og formidle forskning og annen kunnskapsutvikling i spørsmål som berører psykologisk forsvar, og

5. tilrettelegge for samvirke mellom myndigheter og øvrige aktører i det forebyggende arbeidet, samt skape forutsetninger for, og bidra til, å sikre en samordnet operativ utførelse

Myndigheten skal i sin virksomhet verne det åpne og demokratiske samfunnet og den frie meningsdannelsen.

§ 3 Myndigheten skal kunne støtte medieforetak når det gjelder å identifisere, analysere og imøtegå utilbørlig informasjonspåvirkning i den utstrekning slik støtte etterspørres

§ 4 Myndigheten skal bistå regjeringen med underlag for utviklingen av det psykologiske forsvaret i fredstid.

Myndigheten skal, uten opphold, rapportere til regjeringen om utilbørlig informasjonspåvirkning og annen spredning av villedende informasjon som kan ha betydning for Sveriges sikkerhet, eller som regjeringen av andre grunner bør kjenne til.

Hvis Sverige er i krig eller krig truer, skal myndigheten kunne støtte regjeringen og foreslå tiltak innenfor sitt virksomhetsområde som har til hensikt å minske en potensiell angripers evne til, og intensjon for, angrep.

**Ledelse**

§ 5 Myndigheten ledes av en etatssjef («myndighetschef»).

§ 6 Ved myndigheten skal det finnes et tilsynsråd («insynsråd») som består av høyst ti medlemmer.

Embete («anställningar») og oppdrag

§ 7 Generaldirektøren er etatsjef («myndighetschef»)

Personalansvarsnemnd

§ 8 Ved myndigheten skal det finnes en personalansvarsnemnd.

**Anvendelse av andre forskrifter**

§ 9 Myndigheten skal følge personalrepresentantforskriften («personalföreträdarförordningen» (1987:1101).

### 3.1.4 Organisering

Myndigheten for psykologisk forsvar består i skrivende stund av 55 ansatte, med hovedkontor i Karlstad og et kontor utenfor Stockholm. Etaten ledes av en generaldirektør. I ledergruppen sitter generaldirektøren, avdelingssjefene og kommunikasjonssjefen. MPF har tre avdelinger. Beskrivelsen av de ulike avdelingene er hentet fra MPFs nettsider og oversatt til norsk.[16]

**Administrativ avdeling (Administrativa avdelningen)**

Avdelingen sikrer at MPF har en effektiv og rettssikker håndtering av administrative prosesser og gir støtte til hele etaten innen områdene planlegging, oppfølging, økonomi, administrasjon, HR, juss og kommunikasjon.

**Avdeling for kapasitetsbygging (Förmågehöjande avdelningen)**

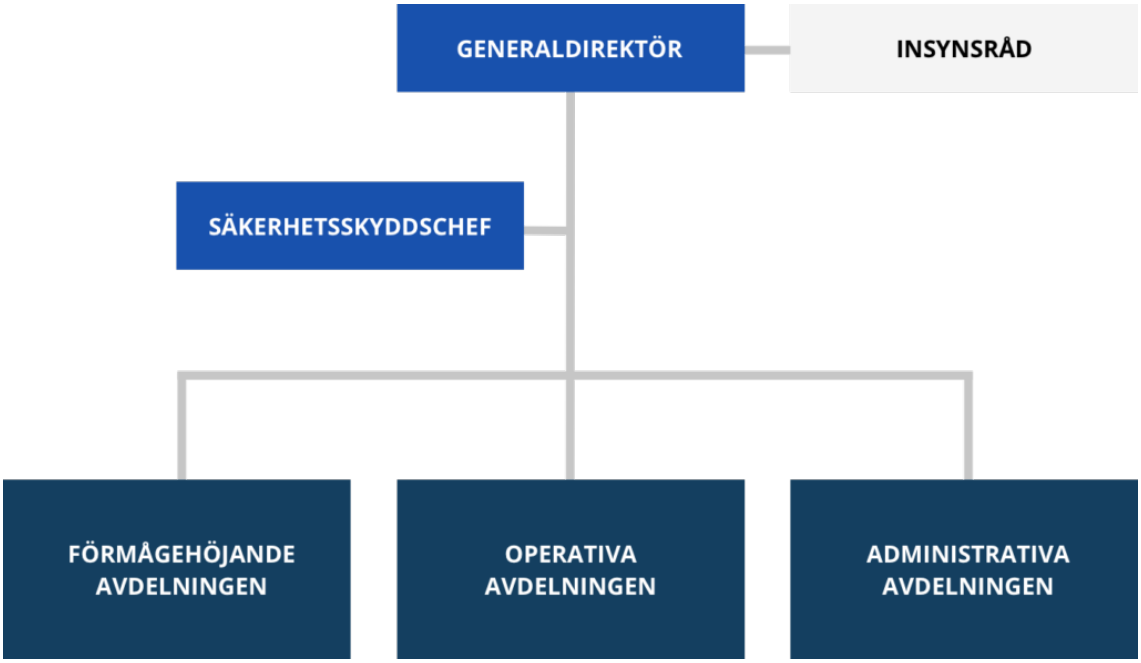
Avdelingen arbeider med å utvikle og styrke samfunnets samlede psykologiske forsvarsevne. I dette inngår å gi støtte til befolkningen, myndigheter, kommuner, media, frivillige forsvarsforeninger og sivilsamfunnet for øvrig, samt tilrettelegge for økt samhandling mellom disse. Viktige oppgaver er også å ta ansvar for utdanning, øving og kunnskapsutvikling, hvilket innebærer å bestille, følge og formidle forskning innen psykologisk forsvar.

**Operativ avdeling (Operativa avdelningen)**

Avdelingen arbeider med å identifisere, analysere og imøtegå utilbørlig informasjonspåvirkning og annen villedende informasjon som er rettet mot Sverige eller svenske interesser. En viktig del av arbeidet er å produsere situasjonsforståelse («lägesbilder»), analyser og rapporter om aktører og aktiviteter som kan utgjøre en trussel mot sårbarheter i samfunnet, samt foreslå relevante mottiltak. Avdelingen utvikler også metoder og teknikker for å identifisere og imøtegå utilbørlig informasjonspåvirkning, i samvirke med andre berørte myndigheter.

**Organisasjonskart**

[16] *Om oss*. Myndigheten för psykologiskt försvar. https://www.mpf.se/om-organisationen/




*Figur 3.1 Organisasjonskart for MPF (fra [https://www.mpf.se/om-organisationen/](https://www.mpf.se/om-organisationen/) ).*

**Innsynsrådet**

Innsynsrådet utpekes av regjeringen og har som oppgave å gi råd til generaldirektøren og føre tilsyn med virksomheten. MPF er en selvstendig myndighet («enrådighetsmyndighet), som innebærer at generaldirektøren er direkte ansvarlig for virksomheten og rapporterer til regjeringen.

Leder i innsynsrådet er p.t. MPFs vikarierende generaldirektør. Rådet består p.t. av ytterligere åtte medlemmer, hvorav tre er stortingspolitikere og de øvrige er representanter fra statlig virksomhet, akademia og privat sektor.

### 3.1.5 Etatsstyring

Regjeringen (Forsvarsdepartementet), styrer *Myndigheten for psykologisk forsvar* gjennom myndighetsinstruksjon og årlige reguleringsbrev. I instruksjonen spesifiseres etatens ansvarsområde og oppgaver (gjengitt her i pkt 3.1.3 Mandat). I reguleringsbrevet spesifiseres mål og rapporteringskrav, samt tildelte ressurser til etatens forvaltning og virksomhet.

### 3.1.6 Utøvelse av virksomheten

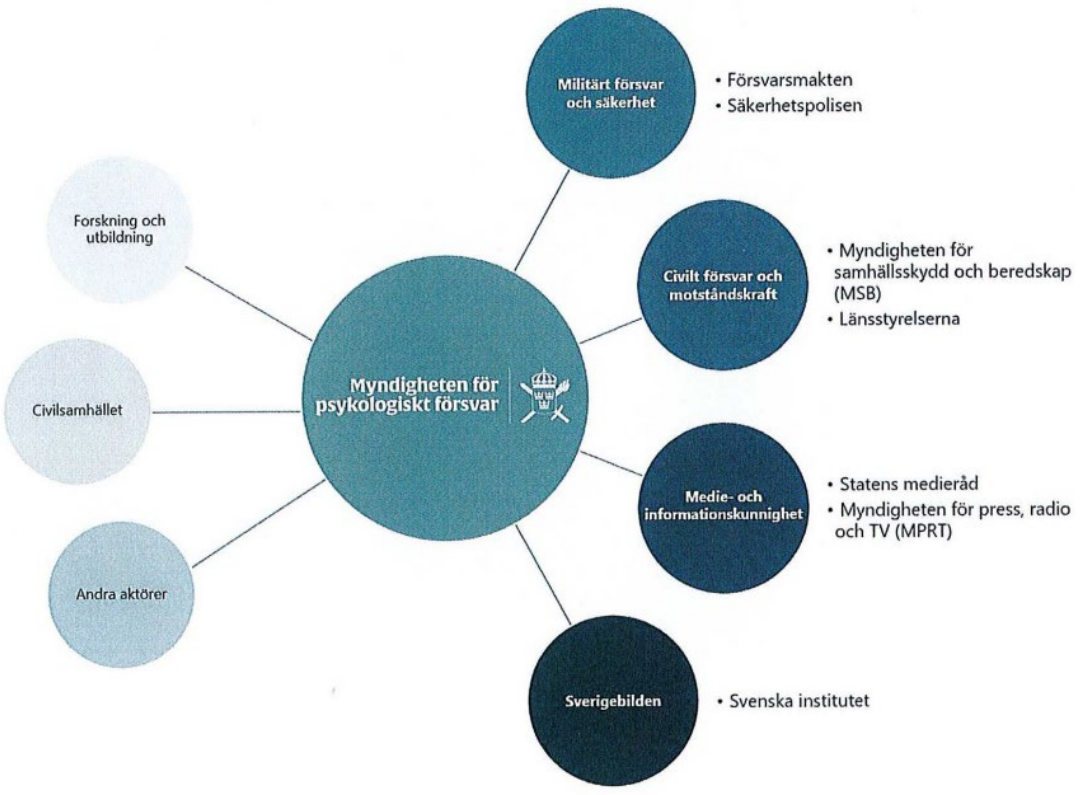
**Samvirkestruktur**

Som ansvarlig for samvirke og koordinering av Sveriges psykologiske forsvar, har MPF identifisert fire virksomhetsområder med relevans for det psykologiske forsvaret:

- Militært forsvar og sikkerhet
- Sivilt forsvar og motstandskraft
- Medie- og informasjonskunnskap
- Sveriges omdømme

I tillegg til disse områdene samarbeider MPF med andre aktører gjennom finansiering av forskning, samordning av aktiviteter og kompetanseheving av sivilsamfunnet.

MPFs samvirkestruktur beskrives som følger (Figur 3.2):




*Figur 3.2 Eksempler på samvirkeområder og etater som inngår i det psykologiske forsvarets samvirkestruktur.*[17]

[17] *Struktur för effektiv samverkan för det psykologiska försvaret*. (2023). Myndigheten för psykologiskt försvar. Rapport MPF/2023:56.

**Forskning og utvikling (FoU)**

MPF har som en del av sitt mandat å følge, bestille og formidle forskning og annen kunnskapsutvikling i spørsmål som berører psykologisk forsvar. Som en del av dette har myndigheten inngått et samarbeid med Lund universitet som har etablert et eget forskningsinstitutt for psykologisk forsvar. Instituttet «utvikler forskningsområdet gjennom å utføre forskning, utvikle strategiske samarbeid med institusjoner på feltet, arrangere seminarer og forskningskonferanser, samt sørge for at forskningsresultater og –trender om psykologisk forsvar formidles til relevante myndigheter og institusjoner».[18]

Etableringen av MPF bygger på både kunnskap og til dels personell fra spesielt to fagmiljøer som har arbeidet med tematikken over tid. Myndigheten för samhällsskydd och beredskap kan sammenlignes med det norske Direktoratet for samfunnssikkerhet og beredskap (DSB). MSBs tidligere oppdrag (og en del personell) innen informasjonspåvirkning er overført til Myndigheten för psykologiskt försvar. MSB har likevel fortsatt en rolle innen Sveriges psykologiske forsvar, primært med å ivareta en kommunikasjonsfunksjon overfor mediene og befolkningen i forbindelse med ulykker, kriseberedskap og totalforsvar.

Totalförsvarets forskningsinstitutt (FOI) ligger under det svenske forsvarsdepartementet og kan sammenlignes med det norske Forsvarets forskningsinstitutt (FFI). Instituttet er en viktig kunnskapsleverandør innen psykologisk forsvar, informasjonspåvirking og desinformasjon som en del av sin forskning på sammensatte/hybride trusler.[19] FOI er en viktig ressurs for MPF.

**Aktiviteter**

MPF har i sitt første virkeår (2022) gjennomført en rekke aktiviteter innenfor sitt virkeområde. De viktigste oppsummeres her[20]:

- Finansiert 15 forskningsprosjekter
- Gjennomført 18 kurs i informasjonspåvirkning
- 3000 personer har deltatt i MPFs kompetanseutviklende virksomhet
- 406 personer har deltatt i MPFs kurs og treninger

https://www.mpf.se/publikationer/#Delredovisning_struktur_for_effektiv_samverkan_for_det_psykologiska_forsvaret

[18] *Forskningsinstitutet för psykologiskt försvar*. Lunds Universitet.
https://www.isk.lu.se/forskning/forskningsomraden/forskningsinstitutet-psykologiskt-forsvar

[19] *Psykologiskt försvar och informationskrigföring.* Totalförsvarets forskningsinstitut.
https://foi.se/forskning/psykologiskt-forsvar-och-informationspaverkan.html

[20] *2022 Årsredovisning*. (2022). Myndigheten för psykologiskt försvar.
https://www.mpf.se/publikationer/#Arsredovisning2022

- Gjennomført én nasjonal kampanje (*Bli inte lurad* ved https://www.bliintelurad.se/)

- Arrangert internasjonal konferanse i Stockholm for 16 land i tillegg til EU, Nato og G7 Rapid Response Mechanism

- Utgivelse av rapporten *Statliga kinesiska påverkansoperationer mot demokratin i svenska kommuner*[21] finansiert av MPF

- Utgivelse av publikasjonen *Att möta informationspåverkan – Handbok för journalister*[22]

- Utgivelse av boka *Skör demokrati : det öppna samhällets motkrafter i svensk offentlig debatt, kultur och forsking*[23] finansiert av MPF

**Operativ effekt**

For å kunne si noe om resultatet av MPFs arbeid så langt, kan det være nyttig å skille mellom «Measures of Performance» (MoP) og «Measures of Effect» (MoE), iht. Natos doktrinelle terminologi. Mens MoP beskriver hvilke tiltak som er gjennomført, beskriver MoE hvilken effekt tiltakene har hatt. Når det gjelder påvirkning, er dette ofte svært krevende å måle. For eksempel viser forskning at økt kunnskap om påvirkning styrker motstandsdyktighet mot å bli påvirket. MPF har, som vist i foregående avsnitt, gjennomført en rekke aktiviteter (MoP) for å øke kunnskap. Hvor mye dette faktisk har styrket motstandsdyktigheten (MoE) er imidlertid svært vanskelig å vite sikkert.

Den operative effekten (MoE) av hendelseshåndtering er imidlertid lettere å beskrive. I sin årsrapport 2022 beskriver MPF å ha levert direkte operativ effekt i forbindelse med konkrete påvirkningsoperasjoner rettet mot Sverige og svenske interesser. MPF har støttet regjeringen, regjeringskanseliet og flere andre myndigheter og fylkesting (länstyrelser) på følgende måte: Deling av situasjonsforståelse, rådgivning for håndtering og konkrete responshandlinger inkludert utvikling av felles talepunkter på strategisk og taktisk nivå. Denne støtten ble gitt både som et resultat av at MPF ble kontaktet av berørte aktører og på MPFs eget initiativ.

Påvirkningsoperasjoner kan være opportunistiske av natur og rettes mot alle samfunnsområder og målgrupper. Gjennom fjoråret fokuserte MPF spesielt på å forebygge og håndtere utilbørlig informasjonspåvirkning på følgende tema og hendelser: Demokratiske valg, det svenske formannskapet i EU, opptakten til og effektene av Russlands fullskala angrep på Ukraina,

[21] Sundqvist, G., et al. (2022). *Statliga kinesiska påverkansoperationer mot demokratin i svenska kommuner.* Myndigheten för psykologiskt försvar. https://www.mpf.se/assets/uploads/2022/11/Statliga-kinesiska-paverkanskampanjer-mot-demokratin-i-svenska-kommuner.pdf
[22] *Att möta informationspåverkan: Handbok för journalister.* (2022). Myndigheten för psykologiskt försvar. https://www.mpf.se/assets/uploads/2022/03/Att-mota-informationspaverkan.pdf
[23] Widman, S., et al (2022). *Skör demokrati: det öppna samhällets motkrafter i svensk offentlig debatt, kultur och forskning*. Fri Tanke. https://www.bokus.com/bok/9789189526709/skor-demokrati-det-oppna-samhallets-motkrafter-i-svensk-offentlig-debatt-kultur-och-forskning/

Sveriges Natosøknad og den islamistiske påvirkningsoperasjonen som ble rettet mot den svenske sosialtjenesten/barnevernet og loven for beskyttelse av barn.

**Kommentar**

Det store spennet i temaer som MPF fokuserte på i 2022, illustrerer hvordan FIMI ikke lar seg definere og håndtere innenfor strenge sektoravgrensninger. Fra et forsvars- og sikkerhetspolitisk ståsted er det åpenbart at både Sveriges Natosøknad og formannskap i EU er av høy betydning for Sverige og svenske interesser. Begge deler kan undergraves gjennom FIMI rettet mot målgrupper både i Sverige og i andre land. Undergravingen kan også være en utilsiktet konsekvens av påvirkning som ikke har noe med disse to forholdene å gjøre i det hele tatt. For eksempel kan Sveriges posisjon i det transatlantiske og europeiske fellesskapet svekkes gjennom svertekampanjene og desinformasjon om den svenske sosialtjenesten, uten at dette var hensikten til den islamistiske bevegelsen som stod bak.

For å fange opp, forstå og håndtere FIMI i sin fulle bredde er det derfor avgjørende at man har god situasjonsforståelse i *hele* informasjonsmiljøet på tvers av sektorer og et fagmiljø som har både kompetansen, mandatet, verktøyene og nettverket til å koordinere både forebygging og responstiltak på, og mellom, nasjonalt og lokalt nivå. Dette er i tråd med mønsterpraksis, som beskrevet i pkt. 2 - Litteraturstudier**.** En eventuell funksjon for forsvarssektoren bør derfor knyttes opp mot en framtidig nasjonal, tverrsektoriell funksjon.

## 3.2 Litauen: Nasjonalt Krisehåndteringssenter og funksjon i Forsvarsdepartementet

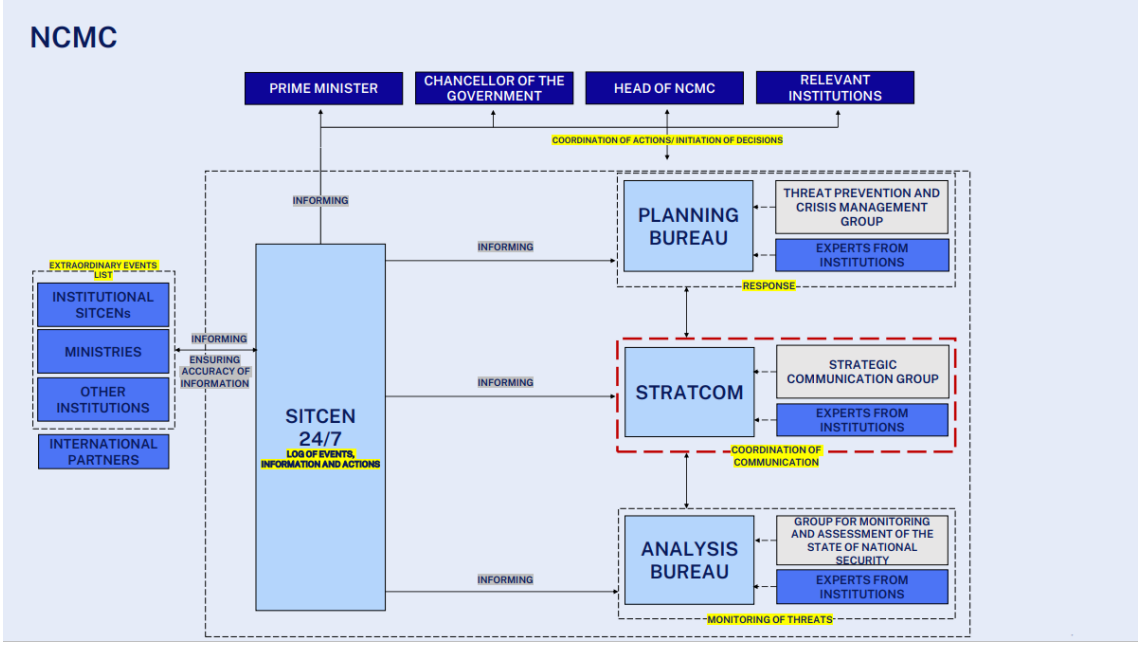
I Litauen finnes en funksjon i form av et nasjonalt krisehåndteringssenter (National Crisis Management Center – NCMC) som samler og koordinerer de statlige etatenes tiltak mot FIMI.

Funksjonen i Litauen hadde sitt utspring i dets væpnede styrker, hvor det ble tydelig at for å sikre statens handlefrihet var det en forutsetning å kunne motvirke fiendens innrykk i IE. De væpnede styrkers kontor ble opprettet i 2009, og startet med å identifisere sårbarheter for FIMI.

Det var også en forståelse for at arbeidet måtte skje åpent. Kontoret la store ressurser i opplysningsarbeid på tvers av samfunnet. Politikere, medier, akademiske institusjoner og offentligheten generelt ble jevnlig informert gjennom presentasjoner, forelesninger og uttalelser. Kontoret delte fritt om fremmedstatlige TTP-er (Teknikker, Taktikker og Prosedyrer), narrativer og avdekte kampanjer.

På grunn av denne offentlige fremgangsmåten fikk flere akademiske institusjoner interesse for FIMI og satte i gang egne prosjekter. Etter hvert spredte dette seg også til myndighetene som tok et mer og mer aktivt grep om problematikken. Aktuelle ministerier fikk egne enheter for strategisk kommunikasjon.

I dag koordineres situasjonsforståelse i IE i Litauen hos det nyopprettede National Crisis Management Center (NCMC). Her finnes et døgnoperativt situasjonssenter som mottar og koordinerer hendelser, informasjon og handlinger innen IE. Alle relevante etater rapporterer til dette senteret, men senteret bedriver også egen innhenting og monitorering. NCMCs struktur belyses av Figur 3.3:

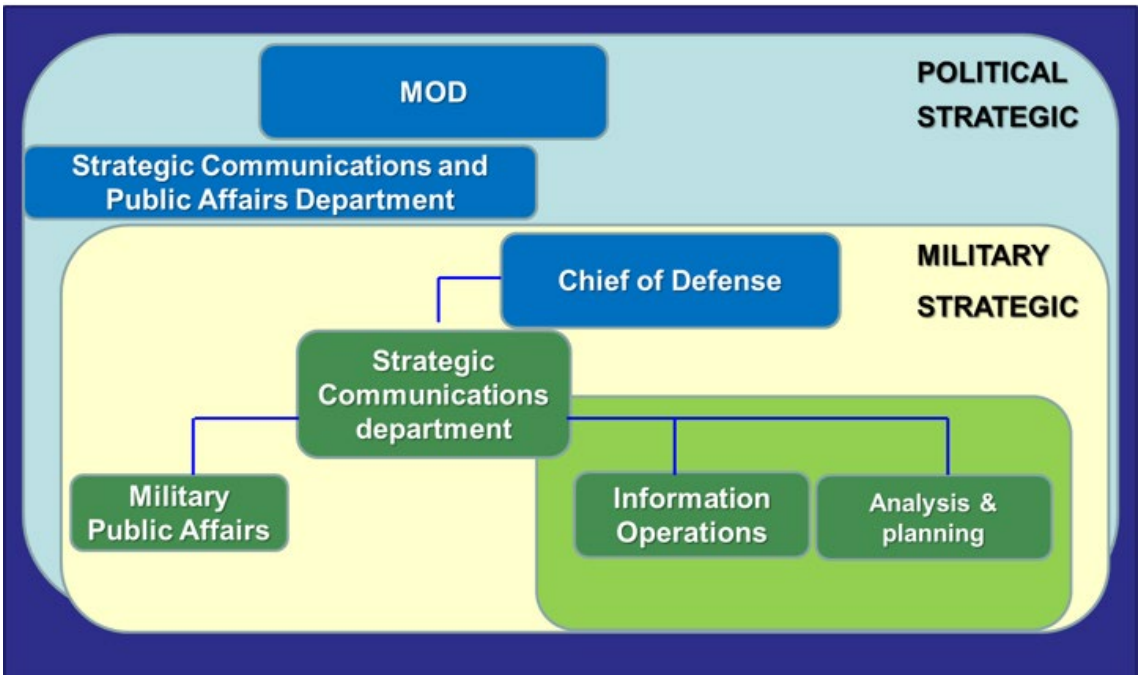



*Figur 3.3 National Crisis Management Center organisasjonsstruktur (fra intervju med NCMC).*

Hver etat benytter egne metoder og verktøy for å fange opp det som er innenfor eget ansvar. Samtidig jobbes det nå med å standardisere dette til en viss grad ved hjelp av EEAS' DISARM-rammeverk og FIMI som konsept.

I Litauen legges det vekt på at nasjonal sikkerhet ligger til grunn for å ha situasjonsforståelse i IE. Det litauiske forsvarsdepartementet beskriver sin rolle som å kontinuerlig måle temperaturen i samfunnet. Deres mål er å øke forsvarsviljen og offentlig støtte til Forsvaret.

Samtidig har kontoret hos Litauens væpnede styrker stadig sin oppgave i behold: å identifisere og motvirke trusler, og å opplyse samfunnet for å styrke befolkningens motstandskraft og avskrekke fremmedstatlige påvirkningsaktører, spesielt Russland. Denne oppgaven er forankret i behovet for å sikre handlingsfrihet. Deres rapporter går gjennom egne linjer og via Forsvarsdepartementet inn i NCMC. Strukturen i det litauiske Forsvarsdepartementet og de væpnede styrkene er beskrevet i Figur 3.4:




*Figur 3.4 Struktur for Litauisk Forsvarsdepartements arbeid mot FIMI (fra intervju med Litauiske Forsvarets Stratkom avdeling).*

Det litauiske eksempelet på en funksjon er nyttig å ta med seg fordi det viser hvordan en funksjon som har utspring i Forsvaret og Forsvarsdepartementet kan fungere, samtidig som det peker mot et overbygg av en struktur som samler modulære, FIMI-rettede kontorer fra andre etater. Samtidig peker erfaringene fra Litauen på fordelene med å rette slike funksjoner etter nasjonal sikkerhet generelt og Forsvarets behov for å ivareta handlefrihet.

# 4 Kontekst til FIMI-forsvar i forsvarssektoren

I dagens sikkerhetspolitiske situasjon, er det et opplagt behov for å kunne forebygge og håndtere FIMI som kan ramme forsvarssektoren og politisk og militær beslutningsevne og handlingsrom. Før vi drøfter hva et slikt FIMI-forsvar i forsvarssektoren skal kunne gjøre og hvordan den kan organiseres, er det nødvendig å se den i sammenheng med Natos tilnærming, alliert samhandling, kobling til Forsvarets operative virksomhet og andre nasjonale aktører.

**Natos eksisterende doktriner**
FIMI, i form av å påvirke virkelighetsoppfattelsen og atferden til ulike målgrupper i krig og væpnet konflikt, er ikke nytt. Nato har egne doktriner og både defensive og offensive kapabiliteter og metoder på dette området, gjennom disiplinene Strategic Communications (STRATCOM), Information Operations (InfoOps) og Psychological Operations (PSYOPS). Dette er imidlertid militære fagdisipliner som ikke kommer til anvendelse i fredstid og utenom militære operasjoner. De har heller ikke til hensikt å beskytte eget sivilsamfunn mot utilbørlig informasjonspåvirkning.

Dette har skapt en utfordring for Nato og alliansens medlemsland. For FIMI rettes i dag mot hele samfunnet på tvers av sektorer, både over og under terskelen for væpnet konflikt. Dette er et eksempel på sammensatte trusler som i stor grad visker ut skillet mellom statssikkerhet og samfunnssikkerhet og terskelen mellom fred, krise og krig. I tillegg utfordrer de det norske sektorprinsippet ved at truslene og effektene er sektorovergripende. Som en konsekvens av det, er det ikke lett å si hvor forsvarssektorens ansvar begynner og slutter.

**Natos fremtidige konsept for kognitiv krigføring**
For å møte denne utfordringen har Nato Allied Command Transformation (ACT) iverksatt et arbeid med å utvikle en konseptuell forståelse for det alliansen kaller «kognitiv krigføring» (Cognitive Warfare). Nato ACTs *Cognitive Warfare Exporatory Concept* er i skrivende stund akkurat ferdigstilt og kan lastes ned (med autorisert tilgang) fra Nato ACT Cognitive Warfare Transnet page. Her defineres Cognitive Warfare som «the activities conducted in synchronization with other instruments of power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage”.[24]

Parallelt leder FFI Nato Science & Technology Organization (STO) sitt FoU-arbeid på kognitiv krigføring for å identifisere og iverksette forskningsaktiviteter for å tette kunnskapshull og utvikle en felles forståelse for hvordan Nato og Natos medlemsland kan beskytte seg. Natos konseptuelle og FoU-baserte arbeid nevnes her fordi et fremtidig konsept for kognitiv krigføring vil inkludere påvirkning i informasjonsmiljøet. Dermed vil dette arbeidet bli en del av konteksten rundt, og stille krav til, et norsk FIMI-forsvar i forsvarssektoren.

**Alliert samhandling**
At Natos arbeid foreløpig ikke er ferdigstilt eller operasjonalisert, står ikke i veien for at medlemslandene etablerer funksjoner og kapabiliteter for å håndtere trusselen fra FIMI i dag. Landene utveksler også informasjon og erfaringer med hverandre i en rekke fora på ulike nivåer. Norges deltakelse her er svært begrenset, da Norge er et av få land som ennå ikke har etablert tilsvarende funksjoner eller operative fagmiljøer.

Nato Stratcom Center of Excellence har etablert to faste møter i året hvor de åtte nordiske og baltiske landene («NB8») oppdaterer hverandre med analyser av sine lands informasjonsmiljø

[24] *Cognitive Warfare: Strengthening and Defending the Mind*. (2023). NATO Allied Command Transformation. https://www.act.nato.int/articles/cognitive-warfare-strengthening-and-defending-mind

og erfaringer med FIMI. Norge er det eneste landet i det nordisk-baltiske fellesskapet som ikke har en fast representant ved Nato Stratcom CoE, og norsk deltakelse i NB8 har så langt vært nedprioritert av Forsvarsdepartementet som i dag ikke har et fagmiljø for å kartlegge, analysere, forebygge eller håndtere FIMI.

Forsvarsdepartementet, sammen med Justis- og beredskapsdepartementet og Utenriksdepartementet, forvalter også norsk deltakelse i The International Partnership to Counter State-sponsored Disinformation (IPCSD). Under jevnlige møter deler deltakerne i denne gruppen erfaringer og lærdommer fra arbeidet med å hindre desinformasjon i sine hjemland, og går samtidig sammen i felleskap for å drive utenlandske kampanjer mot desinformasjon. Ettersom de andre departementene heller ikke har et egnet fagmiljø, har Norge heller ikke her noen jevn representasjon for å dra nytte av og koordinere med andre land.

Etableringen av en funksjon i forsvarssektoren vil derfor ikke bare styrke forsvarssektorens og Norges evne til å håndtere trusler i informasjonsmiljøet, men muliggjøre norsk deltakelse og bidrag inn i en alliert kontekst.

**Kobling til Forsvaret**

Fordi FIMI vil være en del av sikkerhetspolitisk krise og væpnet konflikt, er det nødvendig at en FIMI-funksjon i forsvarssektoren er i stand til å virke i hele krisespekteret i tett samvirke med Forsvaret på operasjonelt nivå.

Forsvarets evne til å operere i informasjonsmiljøet i militære operasjoner er i dag begrenset. FFI anbefaler Forsvaret å etablere evne (kompetanse og dataverktøy) til å oppnå situasjonsforståelse i de virtuelle og kognitive dimensjonene av informasjonsmiljøet (Iht. Nato AJP-3.10 INFOOPS Doctrine). Situasjonsforståelse er en forutsetning for å kunne detektere FIMI, identifisere mottiltak og ha nasjonal kontroll/innflytelse over allierte informasjonsoperasjoner (InfoOps) og -effekter i våre nærområder i en artikkel 5-situasjon.

Forsvarets planverk, operasjonskonsepter og -design bør oppdateres i tråd med Natos nye Joint Doctrine (AJP-1), som nå har en «behaviour centric approach» og "narrative led execution". I tillegg bør Forsvaret oppdatere og/eller implementere doktriner, med tilhørende kapabiliteter, som i varierende grad har vært vektlagt tidligere. Dette gjelder først og fremst AJP-10 (ny STRATCOM-doktrine), AJP 10.1 (revidert INFOOPS doktrine), AJP 10.x (ny Military Public Affairs doktrine p.t. under produksjon), AJP 3.10.1 (revidert PSYOPS-doktrine under produksjon), AJP-3.10.2 (OPSEC & DECEPTION doktrine). INFOOPS bør prioriteres fordi det er en sentral stabsfunksjon og operasjonsmetodikk som koordinerer og synkroniserer aktiviteter fra alle kapabiliteter for å skape ønskede effekter. Disse doktrinene og kapabilitetene, med fagutdannet personell, er viktige for å sikre Forsvarets evne til å drive operasjoner og inngå i allierte fellesoperasjoner som framover vil ha økt vekt på informasjonsmiljøet. De vil også legge grunnlaget for implementering av Natos fremtidige konsept for «Cognitive Warfare».

**Andre nasjonale virksomheter**

Et eget FIMI-forsvar i forsvarssektoren må sees i sammenheng med andre relevante, nasjonale virksomheter. De tre EOS-tjenestene har en rolle i å kartlegge aktiviteter og aktører i informasjonsmiljøet som kan utgjøre en sikkerhetstrussel mot Norge, spesielt Etterretningstjenesten (ETJ). ETJs ansvarsområde er trusler fra fremmede stater og utenlandske organisasjoner og individer og har i oppdrag å innhente, bearbeide og analysere informasjon som er av betydning for Norge og norske interesser. På grunn av utenlandsmandatet, har ETJ begrenset mulighet til å kartlegge FIMI-aktivitet i norske grupper og kanaler på nett og sosiale medier. Den andre begrensningen er at etterretninger som hovedregel er gradert og ikke tilflyter samfunnet.

Politiets sikkerhetstjeneste (PST) har ansvaret for innenlands etterretning, men har foreløpig begrenset evne og mandat til å kartlegge FIMI. Dette kan være i endring. PST vil fra 1. september 2023 få utvidet sine fullmakter til å undersøke påvirkning som kan true nasjonale sikkerhetsinteresser. Det gjenstår å se om PSTs mandat og fremtidige kapasitet vil være tilstrekkelig til å etablere god nok situasjonsforståelse, hvem som vil få tilgang til den og hvordan den vil anvendes. Det er også usikkert i hvor stor grad PST vil, og kan, ha en rolle innen tverrsektoriell forebygging og håndtering. Utvidelsen av PSTs fullmakter har blitt kritisert som inngripende overfor personvernet og for å kunne oppfattes som økt overvåking som kan ha en nedkjølende effekt på det offentlige ordskiftet.[25]

Nasjonal Sikkerhetsmyndighet (NSM) har en viktig rolle i å skape situasjonsforståelse og håndtere hendelser i cyberdomenet, som i stor grad er sammenfallende med den virtuelle dimensjonen i informasjonsmiljøet. NSM har ambisjoner om å ta et større ansvar for å styrke den nasjonale motstandsdyktigheten mot utilbørlig påvirkning, men det er p.t. uklart hva det vil være da arbeidet er pågående. Alle tre tjenestene kan være viktige bidragsytere til et FIMI-forsvar i forsvarssektoren. Det vil imidlertid være viktig å etablere hvordan informasjonsdeling og samvirke skal fungere ikke bare i praksis, men også juridisk og etisk.

En fjerde ressurs er Forsvaret Kommunikasjon (FKOM), tidligere Forsvarets mediesenter, som har en analyseavdeling som i dag monitorerer og analyserer informasjonsmiljøet (redaksjonelle medier og til en viss grad sosiale medier) og som gir daglig klippmappe og medieanalyse til forsvarssektoren. Til sist er både Forsvarsdepartementets kommunikasjonsenhet og presse- og informasjonsapparatet i Forsvaret relevante ressurser.

Et FIMI-forsvar i forsvarssektoren må også sees i en større, nasjonal sammenheng. FFI anbefaler at det etableres et nasjonalt FIMI-forsvar med et tverrsektorielt ansvar. Et eksempel på en slik funksjon er Sveriges *Myndighet for psykologisk forsvar.* Dersom en liknende funksjon på sikt etableres, vil den utgjøre et naturlig faglig oppheng for forsvarssektorens FIMI-forsvar. Sistnevnte kan i en slik organisering være en viktig ressurs for en nasjonal, tverrsektoriell funksjon mot FIMI.

[25] Klepper (2023).

# 5 Krav til FIMI-forsvar i forsvarssektoren

For å identifisere hvilke krav som bør stilles til et FIMI-forsvar i forsvarssektoren, må det først defineres hvilke behov den skal dekke. Vi baserer oss her på mønsterpraksis og Litauens og Sveriges løsninger, samt konteksten beskrevet i foregående kapittel.

Mens Litauen har etablert sine funksjoner med utgangspunkt i FD og Forsvaret og med koordinering med sivile sektorer og aktører, har Sverige etablert en mer sivilt innrettet, egen etat (Myndigheten för psykologiskt försvar) som er underlagt regjeringen ved Forsvarsdepartementet, men frikoblet fra forsvarssektoren (i svensk statsforvaltning styrer regjeringen underliggende myndigheter (etater) gjennom kollektive beslutninger. Den enkelte minister har ikke instruksjonsmyndighet overfor underliggende etater i sin sektor. Svenske etater er mer frittstående enn norske).[26]

I begge land skal funksjonen dekke et behov som går utover forsvarssektorens, fordi FIMI som kan påvirke forsvarssektorens politiske og militære beslutningsevne og handlingsrom kan ha som mål å skape effekter utenfor forsvarssektorens ansvarsområde, som for eksempel ved å undergrave befolkningens tillit til myndighetene generelt eller nasjonens omdømme internasjonalt.

Av samme årsak, legger vi til grunn at et FIMI-forsvar i forsvarssektoren i Norge må ha et bredere blikk enn kun på egen sektor. Vi legger også til grunn at en slik funksjon på sikt skal kunne kobles til en nasjonal, tverrsektoriell funksjon med utgangspunkt i justissektoren, og da kunne forsterke denne.

## 5.1 Hvilke behov skal et FIMI-forsvar dekke?

Basert på mønsterpraksis og Sverige og Litauens løsninger og erfaringer, beskriver vi her hvilke behov funksjonen i forsvarssektoren bør dekke. De presenteres i prioritert rekkefølge. Relevante forvaltningsmessige, organisatoriske, kompetansemessige, tekniske, juridiske og etiske forhold knyttet til å dekke behovene adresseres i kapittel 6.

### 5.1.1 Etablere situasjonsforståelse i informasjonsmiljøet

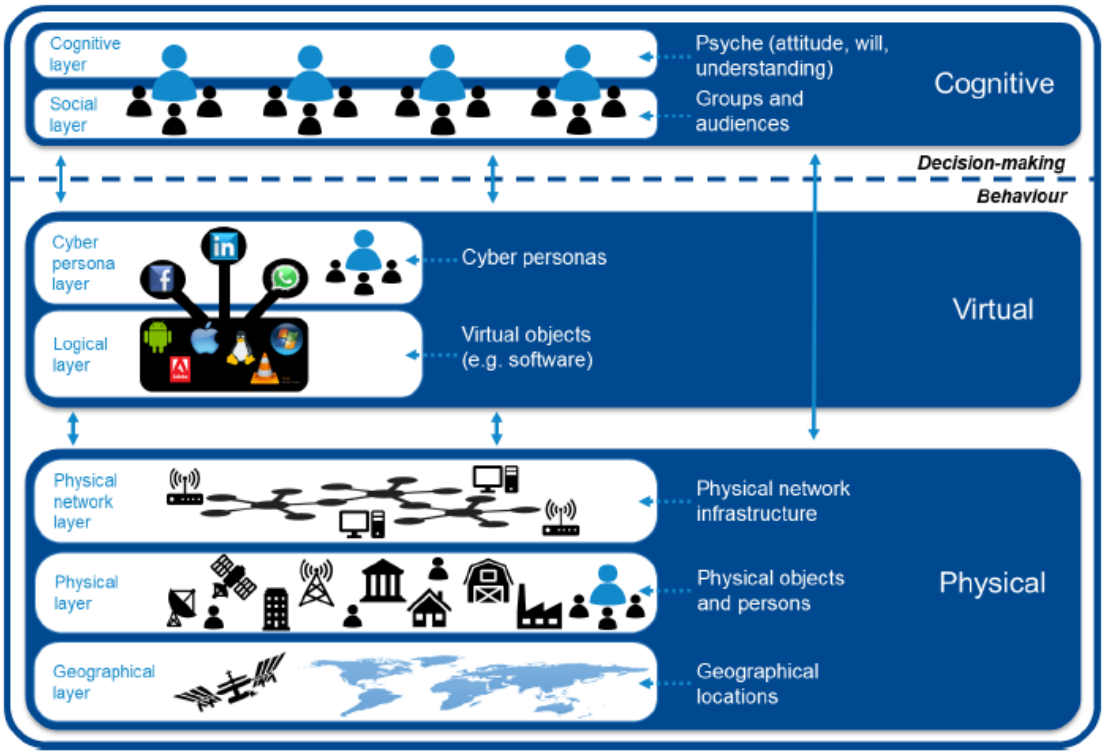
Situasjonsforståelse er en forutsetning for å forstå risiko, avdekke trusler, håndtere hendelser og ta riktige beslutninger. Etter FFIs vurdering er etablering av situasjonsforståelse i informasjonsmiljøet derfor det første og mest grunnleggende behovet FIMI-forsvaret skal dekke.

I Natos doktriner defineres informasjonsmiljøet («Information Environment») som "an environment comprised of the information itself, the individuals, organizations and systems that

[26] *Myndigheter och bolag med statligt ägande*. Regeringskansliet. https://www.regeringen.se/sa-styrs-sverige/myndigheter-och-bolag-med-statligt-agande/

receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs".[27]

Informasjonsmiljøet er komplekst. Følgende illustrasjon søker å beskrive kompleksiteten og sammenhengene gjennom de tre dimensjonene (kognitiv, virtuell og fysisk).




*Figur 5.1 Informasjonsmiljøet ("Information Environment") som beskrevet i Natos Allied Joint Doctrine for Strategic Communications, AJP 3-10.*[28]

De tre dimensjonene er delt inn i lag («layers»). Aktører kan skape effekter i alle tre dimensjonene.

Den kognitive dimensjonen består av holdningene, viljen og forståelsen/virkelighetsoppfattelsen hos mennesker i ulike målgrupper. Eksempler på målgrupper kan være norsk politisk og militær ledelse og beslutningstakere, politikere og den norske befolkningen – eller deler av den.

Den virtuelle dimensjonen består av profiler på sosiale medier og programvare som alt fra operativsystemer og IKT-verktøy/apper til nettsider.

[27] *AJP 3-10. Allied Joint Doctrine for Strategic Communications*. (2023). NATO. s. 7.
[28] Ibid.

Den fysiske dimensjonen består av det som har en fysisk eksistens, som IKT-infrastruktur, tekniske installasjoner, fysiske objekter (inkludert mennesker) og geografisk posisjon.

Det er FFIs vurdering at det er først og fremst i den kognitive dimensjonen og deler av den virtuelle dimensjonen (sosiale medieplattformer og «cyber personas») at norske myndigheter, inkludert forsvarssektoren, i dag ikke har tilfredsstillende situasjonsforståelse. Effekter skapt i den virtuelle og fysiske dimensjonen (f.eks. cyberangrep mot sårbarheter i programvare og sabotasje av IKT-infrastruktur) er erkjent som sikkerhetsrisikoer, og på noen områder også underlagt sikkerhetsloven blant annet gjennom å ha blitt identifisert som grunnleggende nasjonale funksjoner (GNF). Ansvaret for å forebygge, avdekke og håndtere aksjoner mot disse er identifisert og fordelt mellom ulike aktører, som blant annet objekteiere, NSM og – for Forsvarets del – Cyberforsvaret. Sårbarheter i den kognitive dimensjonen og den delen av den virtuelle dimensjonen som handler om sosiale medier er i mindre grad erkjent, analysert og inkludert i risikoreduserende tiltak og ansvarsfordeling i statsapparatet.

*Det er derfor FFIs anbefaling at funksjonen primært bør dekke behovet for situasjonsforståelse i den kognitive dimensjonen og den delen av den virtuelle dimensjonen som omhandler nettbaserte informasjonsplattformer og sosiale medier.*

Samtidig er det viktig å understreke at dimensjonene henger sammen og må forstås i sammenheng med hverandre. For eksempel kan cyberoperasjoner eller sabotasje mot infrastruktur ha som formål å skape effekter i den kognitive dimensjonen. Et eksempel på det er den russiske hackergruppa Killnets tjenestenektangrep mot nettsidene til Arbeidstilsynet, BankID, Altinn, NRK, Schibsted, Nav og politiet i juni 2022. Den tekniske effekten av cyberangrepet var minimal, men angrepet skapte massiv pressedekning som var egnet til å skape frykt og usikkerhet i deler av befolkningen, og som sannsynligvis var hensikten. Slike angrep kan også ha som hensikt å undergrave befolkningens tillit til virksomhetene som blir angrepet, inkludert tillit til systemene og tjenestene deres. Et annet eksempel er hack & release-operasjoner, hvor ekte og/eller forfalsket informasjon fra et datainnbrudd (den virtuelle dimensjonen) lekkes for å påvirke befolkningens eller andre målgruppers virkelighetsoppfattelse eller tillit (den kognitive dimensjonen).

For å skape en mest mulig helhetlig situasjonsforståelse i *hele* informasjonsmiljøet, bør funksjonen løpende utveksle informasjon med aktører som har ansvar for den fysiske (og dels virtuelle) dimensjonen, fortrinnsvis NSM og Cyberforsvaret. Dette for å sikre at alle parter har et mest mulig komplett totalbilde slik at mulige sammenhenger på tvers av dimensjonene kan identifiseres så raskt som mulig. Et tenkt eksempel på det kan være å kunne koble datainnbrudd eller andre cyberoperasjoner med eventuell forsterkende eller formende (shaping) aktivitet i sosiale medier slik at hendelser som er forbundet med hverandre ikke forstås og håndteres som separate hendelser.

### 5.1.2 Detektere forsøk på FIMI

Med etablert situasjonsforståelse på plass, er forutsetningene til stede for å kunne oppdage avvik fra normalsituasjonen og detektere forsøk på FIMI.

*Det er FFIs vurdering at funksjonen må ha evne til å detektere FIMI som kan få betydning for norsk forsvars- og sikkerhetspolitikk, forsvarssektorens oppgaveløsning og politisk og militær beslutningsevne og handlingsrom.*

Eksempler kan være forsøk på å påvirke norske målgruppers holdning til alliert tilstedeværelse, undergrave befolkningens tillit til Forsvaret, nordmenns forståelse av sikkerhetsrisikoer eller Norges omdømme i andre Nato-land. Hvilke temaer og angrepsvektorer funksjonen bør følge med på må utredes på bakgrunn av en risiko- og sårbarhetsanalyse. Det er et eget arbeid som ligger utenfor denne rapportens rammer.

På bakgrunn av mønsterpraksis og FIMIs sektorovergripende natur, bør funksjonen ha evne til å detektere påvirkningsforsøk også på temaer som ikke direkte angår forsvarssektorens ansvarsområde, men som likevel kan få konsekvenser for den. Eksempler kan være utilbørlige forsøk på å svekke tilliten til norske myndigheter generelt og påvirkning som kan true Norges demokratiske styresett.

Å detektere slik aktivitet kan oppleves som overvåkning, og derfor som juridisk og etisk problematisk i et liberalt demokrati. Det er imidlertid fullt mulig å detektere FIMI innenfor rammene av norsk personvernlovgivning, inkludert GDPR. Juridiske og etiske betraktninger beskrives i delkapittel 6.3.

### 5.1.3 Utvikle responsopsjoner for å håndtere FIMI

Når situasjonsforståelse og evne til å detektere FIMI er etablert, er forutsetningene på plass til å kunne håndtere dem i den hensikt å motvirke at de oppnår sin antatte effekt.

Fordi FIMI kan gjennomføres på en rekke ulike måter, rettes mot ulike målgrupper og ha ulike effekter som antatt formål, finnes det ikke én oppskrift på hvordan de skal imøtegås eller hvem som skal ha dette ansvaret. I noen tilfeller kan det handle om å fjerne falske profiler og botnettverk. Da vil NSM, som har en direktelinje til de sosiale medieplattformene, være en viktig aktør å samarbeide med. I andre tilfeller kan det handle mer om å forsøke å redusere de antatte FIMI-effektene ved hjelp av informasjon og råd til de aktuelle målgruppene, inkludert råd og operativ støtte til virksomheter som utnyttes eller er mål i operasjonen.

I enkelte tilfeller vil ikke en symmetrisk respons være mulig eller gi den ønskede effekten. Gjentagende uakseptabel oppførsel som ikke lar seg stoppe gjennom aktive og passive tiltak i informasjonsmiljøet, vil kunne kreve en asymmetrisk respons i et annet domene. En slik asymmetrisk respons kan være økonomiske sanksjoner, forfølge aktører gjennom nasjonale eller overnasjonale domstoler, eller rene militære opsjoner. Norge har et bredt spekter av potensielle responsopsjoner, både alene og sammen med allierte, men denne typen virkemiddelbruk må sees i sammenheng på tvers av tradisjonelle sektorgrenser.[29] Sektorprinsippet i

[29] Skjelland, E., et al. (2023). *Forsvarsanalysen 2023.* FFI-Rapport 23/00659. Forsvarets forskningsinstitutt.

statsforvaltningen har utfordringer i møtet med sammensatte sikkerhetspolitiske trusler som er designet for å utnytte svakhetene i systemet.[30]

Det er FFIs vurdering at FIMI-funksjonen også bør sees i sammenheng med øvrig nasjonal evne til operasjonell og strategisk målbekjemping i fred, krise og krig. Informasjon kan skape egne effekter, eller være en viktig støttefunksjon for å styrke effekten av operasjoner i andre domener eller gjennom bruken av andre maktmidler.

Basert på mønsterpraksis og forskningsfronten, er det rimelig å anta at det i de fleste tilfeller vil være aktuelt og formålstjenlig å offentliggjøre informasjon om hvordan FIMI kan ramme Norge og norske interesser og dele informasjon om FIMI som detektere, inkludert hvem som står bak (hvis kjent og politisk ønskelig) og hvilke effekter de sannsynligvis er ute etter å skape. FIMI-forsvaret vil da ha et ansvar for å dokumentere påvirkningsaktivitetene, utvikle responsopsjoner og rådgi aktuelle norske myndigheter, men ikke nødvendigvis fronte budskap eller håndtere hendelsene selv. Dette vil være en vurdering i hvert enkelt tilfelle og avhenger av hvilket mandat funksjonen får.

*Det er FFIs vurdering at FIMI-forsvaret må kunne bidra til å håndtere FIMI i form av å dokumentere og analysere hendelser og aktiviteter i informasjonsmiljøet, utvikle responsopsjoner, rådgi aktuelle myndighetsorganer og samvirke med andre relevante aktører som blant annet Justis- og beredskapsdepartementet (JD), Nasjonal sikkerhetsmyndighet (NSM), Forsvaret kommunikasjon (FKOM), Forsvarets operative hovedkvarter (FOH), Forsvarsdepartementets kommunikasjonsenhet og avdelinger, samt Etterretningstjenesten (ETJ) og Politiets sikkerhetstjeneste (PST).*

Grenseoppgaven mellom de hemmelige tjenestene, og sannsynligvis andre aktører i statsapparatet, må defineres tydelig og avhenger også av funksjonens mandat.

### 5.1.4 Forebygge FIMI

Forskningsfronten innen FIMI tyder på at forebygging er den mest effektive måten å minimere skadelig FIMI på.[31] Det er også årsaken til at Sveriges *Myndigheten för psykologiskt försvar* holder kurs og informasjonskampanjer rettet mot svenske virksomheter og befolkningen og koordinerer forebyggende tiltak i tillegg til operative. Mens kildekritikk og såkalt «debunking» (motbevise usannheter) av falske nyheter fortsatt er viktig, viser forskning at kunnskap om hvordan påvirkning og manipulasjon gjøres i praksis styrker motstandskraften. En komponent av forebygging er såkalt «prebunking», som – i motsetning til «debunking» gjøres *før* et påvirkningsforsøk, for eksempel ved å informere om at aktør X kan forsøke å fremme påstand Y

[30] Malerud, S., et al. (2021). *Situasjonsforståelse ved sammensatte trusler – et konseptgrunnlag*. FFI-Rapport 21/00246. Forsvarets forskningsinstitutt.
[31] Ullrich, K. H. E. et al. (2022). *The psychological drivers of misinformation belief and its resistance to correction*. Nature Reviews Psychology. https://www.nature.com/articles/s44159-021-00006-y

for å oppnå effekt Z. Denne typen forebygging kan forstås som psykologisk vaksinering mot desinformasjon og annen manipulasjon.[32]

FIMI-forsvaret i Forsvarsdepartementet bør identifisere hva som kan utgjøre en trussel mot sektorens evne til å løse sine oppgaver og ivareta sitt ansvar, men det utøvende ansvaret vil sannsynligvis ligge både i FD og i etatene, så vel som utenfor forsvarssektoren.

For å ta et tenkt eksempel: En fremmedstatlig aktør forsøker å skape et feilaktig inntrykk av at en svært kostbar investering ble besluttet av politikerne for å tekkes USA, ikke vil gi operativ effekt og gå på bekostning av både andre og viktigere anskaffelser og grunnleggende samfunnsfunksjoner som skole og helse. Hvis en stor del av befolkningen tror på et slikt narrativ, kan det forsinke – og i verste fall forhindre – en viktig anskaffelse for norsk forsvarsevne og svekke tilliten både til norske myndigheter, politikere, Forsvarsdepartementet, Forsvaret og Forsvarsmateriell. Hvem har ansvaret for å forebygge at befolkningen tror på et slikt narrativ? I mange tilfeller vil ansvaret ligge på alle involverte. Forsvarsdepartementet og Forsvaret vil ha et ansvar i å få befolkningen til å forstå hvorfor anskaffelsen er nødvendig. Forsvarsministeren og statsministeren vil ha et ansvar i å forklare hvorfor det er riktig å prioritere den over noe annet som også er viktig. Forsvarsmateriell vil ha et ansvar i å skape trygghet for at anskaffelsen er gjort på riktig måte og forklare eventuelle kostnadsoverskridelser. Det samme vil forsvarsministeren. Og alt dette bør gjøres *før* eventuelle FIMI-forsøk inntreffer. Da må sårbarhetene, angrepsvektorene og risikoene identifiseres og forebyggende tiltak utvikles, koordineres og iverksettes. Det er naturlig at en funksjon i forsvarssektoren har det overordnede ansvaret for å sørge for at dette skjer.

*Det er FFIs vurdering at et FIMI-forsvar i forsvarssektoren bør ha et overordnet ansvar for å forebygge effekter av FIMI som kan ramme norsk forsvars- og sikkerhetspolitikk, forsvarssektorens oppgaveløsning og politisk og militær beslutningsevne og handlingsrom. Med dette menes et hovedansvar på strategisk nivå, gjennom å gjennomføre risiko- og sårbarhetsanalyser, sørge for at underliggende etater gjør det samme og koordinere forebyggende tiltak.*

Forebygging skjer ofte gjennom kommunikasjonstiltak. Alle virksomhetene i forsvarssektoren, fra Forsvarsdepartementet til etatene, har egne kommunikasjonsenheter med kommunikasjonsfaglig ekspertise. Et FIMI-forsvar i forsvarssektoren bør derfor ha tett kontakt med Forsvarsdepartementets kommunikasjonsenhet og kommunikasjonsapparatet i etatene. Øvrig beskrives mer om organiseringen i delkapittel 6.1 – organisering.

### 5.1.5 Nasjonal og internasjonal deltakelse og kunnskapsdeling

FIMI er høyt på agendaen i internasjonale fora, både i Nato og EU og multilaterale samarbeidsorganer. Her utveksler deltakerlandene kunnskap gjennom deling av analyser av

[32] Roozenbeek, J. et al. (2022). *Psychological inoculation improves resilience against misinformation on social media*. Science Advances. https://www.science.org/doi/10.1126/sciadv.abo6254

informasjonsmiljøet («Information Environment Analysis»), utvikler strategier og tiltaksplaner for å øke motstandskraften og koordinerer tiltak.

To eksempler hvor behovet er stort er norsk representasjon i Nato Strategic Communications Center of Excellence (Nato Stratcom CoE), hvor Norge i dag ikke deltar og dermed står utenfor Natos kunnskapsdeling. Et annet eksempel er Natos nordisk-baltiske koordineringsforum (Nato NB8), hvor de åtte nordiske og baltiske landene deler kunnskap og erfaringer to ganger i året. Heller ikke her er Norge representert, som det eneste landet, med unntak av deltakelse fra Forsvarets forskningsinstitutt (FFI). Funksjonen kunne også representert Norge ved møter for The International Partnership to Counter State-Sponsored Disinformation (IPCSD).

*FFI anbefaler at FIMI-forsvaret i forsvarssektoren har ansvaret for å representere Norge i relevante fagfora og, når relevant, produsere kunnskapsgrunnlaget til andre norske representanter, både politikere og byråkrater, som deltar i møter og fora hvor påvirkningsoperasjoner står på agendaen.*

## 5.2 Prinsipper for et FIMI-forsvar

I foregående delkapittel beskrives hvilke behov et FIMI-forsvar i forsvarssektøren bør dekke. Disse er, kort oppsummert: Å etablere situasjonsforståelse i informasjonsmiljøet, detektere forsøk på FIMI, utvikle responsopsjoner for å håndtere FIMI og sikre nasjonal og internasjonal deltakelse og kunnskapsdeling i relevante fora.

I det følgende beskrives kort hvilke prinsipper FFI vurderer bør ligge til grunn for et FIMI-forsvar i forsvarssektoren.

a) Må ha solid hjemmelsgrunnlag.

    - Sikrer legitimitet for en aktivitet som kan være gjenstand for etiske og juridiske spørsmål. Kan også brukes for å befeste grunnlaget for funksjonen innen for eksempel nasjonal sikkerhet.

b) Må være kompatibel med Nato-standarder (InfoOps og Stratcom-doktrinene).

    - Sikrer interoperabilitet og bygger på allerede etablert kunnskap og praksis.

c) Må være skalerbar for å kunne utvikles i takt med behov.

    - FIMI er et raskt skiftende fenomen og har som forutsetning den hurtige teknologiske utviklingen. I tillegg vil det være naturlig å forvente forskjeller i volum på fiendtlig FIMI i takt med valg, offentlige debatter og nasjonale og internasjonale hendelser.

d) Må være fleksibel nok til å tilpasse seg løpende endringer i aktør- og trusselbilde, herunder endringer i metoder og virkemidler.

- Som over. Utviklingen av sosiale medier, teknologi og sosiale trender, samt utviklingen i den sikkerhetspolitiske situasjonen kan endre forutsetninger for hvordan FIMI gjennomføres, og av hvem.

e) Må samvirke med de andre aktørene i forsvarssektoren, primært FOH og etatene.

   - Sikrer bred informasjonsutveksling og nyttegjøring av analyser i begge retninger. Forankrer også funksjonen bredt i sektoren.

f) Må samvirke med andre sivile aktører som JD og UD primært, men også hele statsapparatet (f.eks. ta inn personell fra relevante sektorer ved behov – som da Helse ble med i Depstrat under pandemien).

   - FIMI er en sektorovergripende trussel. Prinsippet sikrer bred samhandling med relevante aktører, og vil bidra til å inspirere andre aktører til å ta trusselen på alvor.

g) Bør ikke oppleves som overvåkning av nordmenn.

   - Dette er en fallgruve for en slik funksjon, og det bør gjøres et grundig kommunikasjonsarbeid for å opplyse om funksjonens mandat, hvordan den arbeider og hva den gjør for å ivareta personvern og ytringsfrihet. Åpenhet om det løpende arbeidet, inkludert analyser og funn, vurderes som avgjørende for å sikre både demokratisk forankring og effekt.

h) Bør ikke være 100% avhengig av verktøy som ikke er under nasjonal kontroll.

   - Ettersom funksjonen vil tas i bruk for å sikre grunnleggende nasjonale funksjoner for Forsvaret og forsvarssektoren (sikre Forsvarets og Norges handlingsfrihet), bør den ikke være avhengig av utenlandske verktøy som kan falle fra, begrenses eller kompromitteres. Det er likevel vanskelig å komme utenom kommersielle verktøy, så sårbarhetsanalyser og beredskapsplaner bør utvikles for tilfeller hvor disse ikke lenger kan brukes.

i) Bør ikke utfordre andre sektorers/etaters ansvarsområder, men støtte disse.

   - Sektorprinsippet står sterkt i Norge, og for å bygge opp funksjonens verdi for nasjonens sikkerhet bør den ikke utfordre dette. Det bør heller legges opp til proaktiv deling og koordinering på tvers av sektorer.

j) Bør unngå "duplication of effort" med aktører som PST, NSM og ETJ, og heller søke å skape synergieffekter så langt det er juridisk mulig og etisk tilrådelig.

   - EOS-tjenestene vil være en naturlig partner til funksjonen, og arbeidsporteføljer bør være klart skilt. Et overlapp av oppgaver vil være ineffektivt men også

kunne skape unødig konflikt mellom tjenestene og funksjonen. Det er viktig at åpenhet og demokratisk forankring at funksjonen i forsvarssektoren ikke skal, eller oppfattes å, drive med etterretning.

k) Bør kunne videreutvikles eller brukes som utgangspunkt for en annen organisering og oppheng i framtiden.

    - Som nevnt er FIMI et tverrsektorielt fenomen, hvor forsvarssektoren er en betydelig men ikke enerådende arena. Å bygge funksjonen med tanken om at det vil kunne etableres en bredere funksjon senere vil oppfordre til dette og sikre en smidig innfasing om så skulle skje.

l) Bør kommunisere tydelig begrunnelsen for å begynne i forsvarssektoren, med behov for oppheng sivilt.

    - Funksjonen har sitt utspring i forsvarssektoren fordi FIMI kan utgjøre en trussel mot nasjonal sikkerhet. Samtidig bør ikke etableringen av funksjonen gi inntrykk av at forsvarssektoren ser på FIMI som sin oppgave alene, men anerkjenne fenomenets tverrsektorielle natur og oppfordre til liknende initiativer der de er fornuftige. En fremtidig sivil, tverrsektoriell FIMI-funksjon vil kunne være et naturlig oppheng for FIMI-funksjoner i alle sektorer, inkludert forsvarssektorens FIMI-forsvar.

# 6 FIMI-forsvarets organisering, struktur, og etiske betraktninger

## 6.1 Organisering

Hvordan FIMI-forsvaret organiseres innen sektoren er i stor grad utenfor FFIs ekspertise. Allikevel, med henblikk på de foregående kapitlene er det mulig å gi en pekepinn på det som kan se ut som en fornuftig organisering og et logisk oppheng.

Av litteraturstudiene kommer det frem at det er nyttig med nok autoritet til å kunne være førende med standarder, verktøy og praksis. Det vil også være en fordel å enkelt kunne dele informasjon og samarbeide med andre etater i og utenfor sektoren.

I Sveriges tilfelle er MPF organisert på en måte som gir mye autoritet og bred mulighet for å snakke med andre etater. Organiseringen her gir myndigheten også kort vei til beslutningstakere

og en god koordineringsposisjon. I Litauens eksempel er disse fordelene ivaretatt av koordineringssenteret, hvor funksjonen i forsvarssektoren spiller en stor rolle.

Konteksten for en slik funksjon i forsvarssektoren beskriver de aktørene og den situasjonen funksjonen kommer inn i. Organiseringsmessig bør det her legges vekt på samarbeidsmuligheter mellom de ulike aktørene beskrevet.

Det er omfattende krav til en slik funksjon, som igjen peker på nødvendigheten av en sterk forankring der den kan fungere effektivt. Funksjonens oppgaver omfatter store aktivitetsområder for forsvarssektoren, som deteksjon, forebygging, etablering av situasjonsforståelse, utvikling av respons, og bør følge prinsipper som omhandler koordinering, riktig forankring og godt samvirke, blant andre. Dette illustrerer også fordelen med å opprette en slik funksjon på et hensiktsmessig nivå i organisasjonen.

## 6.2 Struktur

Funksjonens struktur er avhengig av mange faktorer utenfor denne analysen, som finansiering, endelig mandat, hjemmelsgrunnlag og så videre, men basert på de foregående kapitlene kan man utlede noen indikasjoner på hvordan den bør se ut.

Litteraturstudien peker på behovet for en struktur som bygger samhandling gjennom de ulike kapabilitetene i funksjonen. Spesielt analyse-elementet bør virke på tvers av hele funksjonen. Det bør også legges opp til en struktur som kan koordinere og samvirke med enheter og etater utenfor funksjonen på en effektiv måte.

I case-studiene om Sverige og Litauen belyses mulige strukturer som det kan dras inspirasjon fra. Sveriges MPF har tre avdelinger (kapasitetsbygging, operativ, og administrasjon), mens i Litauen skilles det mellom administrasjon/planlegging (herunder også kapasitetsbygging), operasjoner og til dels analyse.

Det synes fordelaktig å ha en struktur som enkelt kan forstås og bidrar til samvirke med andre etater og enheter, og som fyller de behovene konteksten belyser.

Strukturen bør i tillegg speile de behov funksjonen skal svare ut, beskrevet i kapittel 5. Det vil si å etablere situasjonsbilde, detektere trusler, utvikle responser, forebygge mot mulige trusler og dele kunnskap nasjonalt og internasjonalt. Ifølge prinsippene i punkt 5.2, bør også strukturen kunne skaleres og oppleves fleksibel i møte med endrede trusselbilder.

## 6.3 Etikk og jus

Kanskje en av de største utfordringene med å etablere tiltak mot FIMI er de etiske og juridiske problemstillingene som oppstår. Samfunnsdebatten dreier seg med hurtighet mot prinsipper som ytringsfrihet og privatliv, og hvordan disse kan svekkes i kampen mot FIMI.

Det er ikke gjort en grundig utredning av lover og regler i dette arbeidet. Men tidligere FFI-rapporter har pekt på utfordringene som oppstår i det å praktisk arbeide mot FIMI. Det foreligger for eksempel et lovforslag om å gjøre samarbeid med fremmede etterretningstjenester rundt påvirkningsvirksomhet ulovlig. Selv om dette kan bidra noe til informasjonsutveksling mellom EOS-tjenestene vurderes det at «siden fremmedstatlige påvirkningsoperasjoner først og fremst gjennomføres fra utlandet og av utenlandske borgere, er det usikkert hvor stor effekt en slik hjemmel vil ha.»[33] I tillegg har lovforslaget høstet kritikk for å stride mot personvernsbestemmelser.

Som poengtert tidligere i punkt 5.2 må funksjonen ha et grundig etablert og solid hjemmelsgrunnlag, nettopp for å møte disse utfordringene. Det gjelder både å innrette funksjonen slik at den effektivt kan utgjøre sine oppgaver og å imøtekomme bekymringer fra andre etater og samfunnet generelt.

Det er tydelig at FIMI-forsvaret må ha mandat til å samle inn, lagre og analysere data. Både Etterretningstjenesten og PST har, med henholdsvis ny Etterretningslov og endringer i Politiforskriften, fått større muligheter for dette. Allikevel vil et tenkt FIMI-forsvar i forsvarssektoren med liten sannsynlighet falle inn under Etterretningsloven eller Politiforskriften. Spørsmålet blir dermed hvilket hjemmelsgrunnlag en slik funksjon kan legge til grunn for sin virksomhet, om det per dags dato finnes en juridisk mulighet til dette eller om det er behov for noe nytt. Svar på slike spørsmål er det fortrinnsvis andre enn FFI som er mer egnet til å gi.

# 7 Anbefaling for etablering av FIMI-forsvar i forsvarssektoren

Følgende anbefaling er utledet av mønsterpraksis, erfaringene fra Sverige og Lituauen og de vurderingene beskrevet hittil i denne rapporten.

FFI anbefaler at et FIMI-forsvar har ansvar for å:

1. Etablere situasjonsforståelse i informasjonsmiljøet
2. Detektere, utvikle responsopsjoner til og forebygge mot FIMI
3. Ivareta nasjonal og internasjonal deltakelse og kunnskapsdeling i relevante fora.

[33] Klepper (2023), s. 67.

FFI anbefaler at Forsvarsdepartementet selv vurderer hvor en slik funksjon skal etableres.

FFI anbefaler at funksjonen bygger analytisk kapasitet som grunnlag i arbeidet, og tilegner seg personell med kompetanse innen blant annet: risiko og sårbarhetsanalyser, sosiale medier analyser, OSINT, sammensatte trusler, strategisk kommunikasjon, informasjonsoperasjoner, og psykologiske operasjoner. FDs Kommunikasjonsenhet bør også representeres i funksjonen for å ivareta strategisk kommunikasjon og bidra med kommunikasjonsekspertise.

FFI anbefaler at det utarbeides et omforent mandat for funksjonen.

FFI anbefaler en egen utredning av digitale verktøy for analyse som svarer til funksjonens behov. Det vil være nødvendig med verktøy som kan utføre OSINT, jobbe med stordata og nettverksanalyser, og detektere koordinert, inautentisk atferd. Verktøyet bør kunne tilpasses skiftende behov.

FFI anbefaler en egen utredning om et mulig hjemmelsgrunnlag for funksjonen.

FFI anbefaler at funksjonen bygges for å i fremtiden kunne samvirke med en større, tverrsektoriell funksjon.

# Referanser


*1st EEAS Report on Foreign Information Manipulation and Interference Threats – Towards a framework for networked defence*. (2023). European External Action Service. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

*2022 Årsredovisning*. (2022). Myndigheten för psykologiskt försvar. https://www.mpf.se/publikationer/#Arsredovisning2022

*Academic & Think Tank Highlights*. (2021). Global Engagement Center Academic & Think Tank Outreach Unit. (Unclassified).

*AJP 3-10. Allied Joint Doctrine for Strategic Communications*. (2023). NATO.

*Att möta informationspåverkan: Handbok för journalister.* (2022). Myndigheten för psykologiskt försvar. https://www.mpf.se/assets/uploads/2022/03/Att-mota-informationspaverkan.pdf

Bergaust, J. C., Skjei, F. & Sellevåg, SR. (2022). *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? – rapport til Forsvarskommisjonen*. FFI-rapport 22/02310. Forsvarets forskningsinstitutt.

*Best Practices in Detecting and Analysing Foreign State Online Manipulation*. (2020). The Institute for Strategic Dialogue.

Buvarp, P. M. H. (2023) *International Partnership to Counter Statesponsored Disinformation Meeting Participation, January 2023 ─ Meeting summary with detailed appendices*. FFI-Notat 23/00718. Forsvarets forskningsinstitutt. (U. Off.)

*Cognitive Warfare: Strengthening and Defending the Mind*. (2023). NATO Allied Command Transformation. https://www.act.nato.int/articles/cognitive-warfare-strengthening-and-defending-mind

Ds 2014:20. (2014). *Försvaret av Sverige - Starkare försvar för en osäker tid.* Försvarsberedningen. https://www.regeringen.se/rattsliga-dokument/departementsserien-och-promemorior/2014/05/ds-201420/

*Forskningsinstitutet för psykologiskt försvar*. Lunds Universitet. https://www.isk.lu.se/forskning/forskningsomraden/forskningsinstitutet-psykologiskt-forsvar

Klepper, K. B., Bentstuen, O. I., Bergh, A., Broen, T., Kveberg, T., Lindgren, P. Y., Sivertsen, E. G., Sjøvik, Ø., Svenes, K., Waage, K., & Windvik, R. (2023) *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv*. FFI-rapport 23/00879. Forsvarets forskningsinstitutt.

Kommittédirektiv 2021:936. (2021). *Förordning (2021:936) med instruktion för Myndigheten för psykologiskt försvar.* https://riksdagen.se/sv/dokument-lagar/dokument/kommittedirektiv/forordning-2021936-med-instruktion-for_H9B1936

Malerud, S., Hennum, AC., & Toverød, N. (2021). *Situasjonsforståelse ved sammensatte trusler – et konseptgrunnlag*. FFI-Rapport 21/00246. Forsvarets forskningsinstitutt.

*Myndigheten för psykologiskt försvar.* Myndigheten för psykologiskt försvar. https://www.mpf.se

- *Om oss*. Myndigheten för psykologiskt försvar. https://www.mpf.se/om-organisationen/

- *Uppdraget*. Myndigheten för psykologiskt försvar. https://www.mpf.se/vart-uppdrag/

*Myndigheten för samhällsskydd och beredskap*. Myndigheten för samhällsskydd och beredskap. https://www.msb.se/

*Myndigheter och bolag med statligt ägande*. Regeringskansliet. https://www.regeringen.se/sa-styrs-sverige/myndigheter-och-bolag-med-statligt-agande/

NOU 2023:14. (2023). *Forsvarskommisjonen av 2021 — Forsvar for fred og frihet*. regjeringen.no/contentassets/8b8a7fc642f44ef5b27a1465301492ff/no/pdfs/nou202320230014000dddpdfs.pdf.

*Psykologiskt försvar och informationskrigföring.* Totalförsvarets forskningsinstitut. https://foi.se/forskning/psykologiskt-forsvar-och-informationspaverkan.html

Roozenbeek, J., Van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). *Psychological inoculation improves resilience against misinformation on social media*. Science Advances. https://www.science.org/doi/10.1126/sciadv.abo6254

Skjelland, E., Arnfinnsson, B., Birkemo, G. A., Bråthen, K., Glærum, S., Graarud, E., Hakvåg, U., Klepper, K. B., Kvalvik, S. N., Larsen, M. V., Mayer, M. J., Minos-Stensrud, M., Monsen, I. H. L., Mørkved, T., Nordvang, E. U., Presterud, A. O., Sellevåg, SR., Sendstad, C., Sivathas, K., Strand, K. R., Thuv, Å., & Voldhaug, JE.. (2023). *Forsvarsanalysen 2023.* FFI-Rapport 23/00659. Forsvarets forskningsinstitutt.

SOU 2020:29. (2020). *En ny myndighet för att stärka det psykologiska försvaret.* Statens Offentliga Utredningar. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2020/05/sou-202029/

*Struktur för effektiv samverkan för det psykologiska försvaret*. (2023). Myndigheten för psykologiskt försvar. Rapport MPF/2023:56. https://www.mpf.se/publikationer/#Delredovisning_struktur_for_effektiv_samverkan_for_det_psykologiska_forsvaret

Sundqvist, G., & Lindberg, F. (2022). *Statliga kinesiska påverkansoperationer mot demokratin i svenska kommuner.* Myndigheten för psykologiskt försvar. https://www.mpf.se/assets/uploads/2022/11/Statliga-kinesiska-paverkanskampanjer-mot-demokratin-i-svenska-kommuner.pdf

Ullrich, K. H. E., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K., & Amazeen, M. A. (2022). *The psychological drivers of misinformation belief and its resistance to correction*. Nature Reviews Psychology. https://www.nature.com/articles/s44159-021-00006-y

Widman, S., & Persson, T. (2022). *Skör demokrati: det öppna samhällets motkrafter i svensk offentlig debatt, kultur och forskning*. Fri Tanke. https://www.bokus.com/bok/9789189526709/skor-demokrati-det-oppna-samhallets-motkrafter-i-svensk-offentlig-debatt-kultur-och-forskning/

## Om FFI

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

## FFIs formål

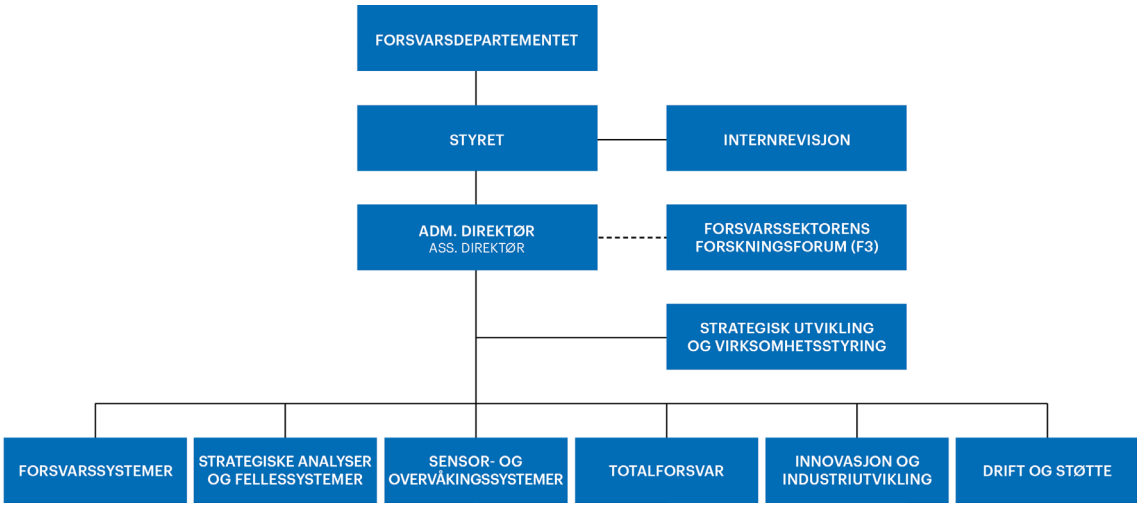
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en