FFI Forsvarets forskningsinstitutt

22/02310

FFI-RAPPORT

Hva kan Norge lære av andre lands tilnærming til sammensatte trusler?

– rapport til Forsvarskommisjonen

Julie Celine Bergaust
Frida Skjei
Stig Rune Sellevåg

Hva kan Norge lære av andre lands tilnærming til sammensatte trusler?
– rapport til Forsvarskommisjonen

Julie Celine Bergaust
Frida Skjei
Stig Rune Sellevåg

Forsvarets forskningsinstitutt (FFI) 15. november 2022

Emneord
Internasjonal politikk
Sikkerhetspolitikk
Trusler
Hybridkrigføring
Nasjonal sikkerhet
Samfunn og sikkerhet

FFI-rapport
22/02310

Prosjektnummer
1619

Elektronisk ISBN
978-82-464-3438-4

Engelsk tittel
What can Norway learn from other states' approach to hybrid threats? – A report to the Norwegian Defence Commission

Godkjennere
Janet Martha Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Forsvarskommisjonen av 2021–2023 skal vurdere sikkerhets- og forsvarspolitiske veivalg og prioriteringer for Norge i et 10–20-årsperspektiv. Som en del av denne vurderingen har Forsvarets forskningsinstitutt (FFI) fått i oppdrag å vurdere hva Norge kan lære av Finland, Sverige, Estland, Storbritannia, Nederland og Australia når det gjelder disse landenes arbeid med å avskrekke, avdekke og håndtere sammensatte trusler. Rapporten belyser hva som er foreslått mønsterpraksis for Nato og EU og hvordan de forskjellige landene i studien har tilnærmet seg sammensatte trusler. I beskrivelsen av landene i studien gis en ikke-uttømmende liste over aktuelle og relevante tiltak som er igangsatt eller foreslått igangsatt – men det er ikke gjort egne undersøkelser om hvorvidt tiltakene faktisk fungerer. På bakgrunn av foreslått mønsterpraksis, og de ulike landenes tilnærminger, er det gitt en vurdering av hva Norge kan lære for å styrke evnen til å avskrekke, avdekke og håndtere sammensatte trusler.

Basert på denne studien gir FFI følgende anbefalinger til Forsvarskommisjonen:

(*i*) Enighet om begrepsbruk og forståelse er avgjørende for god situasjonsforståelse. FFI anbefaler at Forsvarskommisjonen tar utgangspunkt i Forsvarsdepartementets definisjon, men forståelsen bør videreutvikles for å kunne utvikle politikk som skiller mellom forskjellige typer aktiviteter, intensitetsnivå på innblandingen og alvorlighetsgrad.

(*ii*) Foreslått mønsterpraksis og andre lands tilnærminger fremhever at nasjonal håndtering må være synkronisert, systematisk og tilpasset. Forsvarskommisjonen bør se nærmere på hvordan en helhetlig og proaktiv samfunnstilnærming, med evne til synkronisert, systematisk og tilpasset håndtering, kan innrettes. Som en del av dette bør Forsvarskommisjonen vurdere nærmere et helhetlig nasjonalt forsvars- og sikkerhetskonsept.

(*iii*) Forsvarskommisjonen bør vurdere hvordan en strategisk funksjon for å styrke regjeringens situasjonsforståelse kan innrettes, hvordan norske etterretnings- og sikkerhetstjenester kan styrkes og om det er behov for å endre dagens struktur for innenlands- og utenlandsetterretning.

(*iv*) Det største handlingsrommet Norge har som et liberalt demokrati er å styrke motstandsdyktigheten i vårt demokrati, kritiske samfunnsfunksjoner og i befolkningen. Forsvarskommisjonen bør vurdere hvordan et moderne psykologisk forsvar kan innrettes i Norge.

(*v*) For å ivareta rettssikkerhet, demokrati og menneskerettigheter bør rettslige tiltak vurderes å være smale for å unngå at tiltakene en igangsetter går på bekostning av verdiene en forsøker å beskytte. Forsvarskommisjonen bør se nærmere på tiltak som fremmer åpenhet.

(*vi*) Det bør utøves aktsomhet med hensyn til mulige utvidelser av Forsvarets ansvar knyttet til å avskrekke, avdekke og håndtere sammensatte trusler. Forsvarets viktigste oppgaver vil være å opprettholde evne til militær avskrekking, bidra med etterretning, ha situasjonsforståelse i domener hvor Forsvaret har unike kapasiteter, samt bistå sivile myndigheter med å ivareta samfunnssikkerheten.

Summary

The Norwegian Defence Commission of 2021–2023 shall assess security and defence choices and priorities for Norway in a 10–20 year perspective. As part of this assessment, the Norwegian Defence Research Establishment (FFI) has been commissioned to consider what Norway can learn from Finland, Sweden, Estonia, the United Kingdom, the Netherlands and Australia regarding how they work to deter, detect and respond to hybrid threats.

The report sheds light on suggested best practices in Nato and the EU, and how the different states have approached the topic of hybrid threats. A non-exhaustive list of relevant measures is presented. We have not undertaken examinations on the effectiveness of the measures. Based on the suggested best practices and the states' approaches, recommendations regarding what Norway can learn to strengthen the ability to counter hybrid threats is given.

Based on this study FFI gives the following recommendations to the Defence Commission:

(*i*) Clarification of concepts and terms is decisive for situational awareness. The Defence Commission should use the Ministry of Defence's definition for the purpose of their mandate, but the conceptual understanding of hybrid threats should be advanced to develop policies that differentiate between different activities, level of intensity, and degree of severity.

(*ii*) Suggested best practices and other states' approaches highlights that national handling must be syncronised, systematic and customized. The Defence Commission should look further into how a proactive and whole-of-society approach – with the ability to act syncronised, systematic and customized – can be organised. As part of this, the Defence Commission should consider a comprehensive national security and defence concept.

(*iii*) The Defence Commission should consider how a strategic function to strengthen the Norwegian government's situational awareness could be organised, how the Norwegian intelligence and security services can be strengthened, and whether today's structure for domestic and foreign intelligence should be modified.

(*iv*) The largest room for development in Norway as a liberal democracy is to strengthen resilience in our democracy, in critical infrastructure and in the population. The Defence Commission should consider how a modern psychological defence could be organised in Norway.

(*v*) Legal changes ought to be considered to be narrow, in order to take care of rule of law, democracy and human rights, and ensure that the measures initiated to protect our values are not at the expense of the same values we seek to protect.

(*vi*) Caution should be exercised regarding possible expansions of the Norwegian Armed Forces' responsibility related to countering hybrid threats. The Armed Forces' most important task is to maintain military capacity for deterrence, contribute to situational awareness and assist civilian authorities with maintaining societal security.

Innhold

Forord

I dette oppdraget har Forsvarets forskningsinstitutt (FFI) gjennomført en utredning vedrørende ulike lands tilnærming til håndtering av sammensatte trusler. Vi har sett på systemer for tverrsektoriell situasjonsforståelse, sivil-militært samarbeid, situasjonsforståelse og gjennomførte tiltak i Finland, Sverige, Estland, Nederland, Storbritannia og Australia. Tiltakene i de ulike landene har blitt vurdert opp mot mønsterpraksis.

Studien er gjennomført på oppdrag fra Forsvarskommisjonen av 2021–2023. Rapportens vurderinger og anbefalinger er derfor skrevet med tanke på at de skal være nyttige for Forsvarskommisjonens arbeid. Rapporten er således ikke konkluderende og vurderingene som rapporten gir, er heller ikke førende for kommisjonens arbeid.

For å kunne fremskaffe et så godt kunnskapsgrunnlag som mulig innenfor den begrensede tiden som var tilgjengelig for oppdraget, har FFI valgt å benytte egne økonomiske ressurser i tillegg til finansieringen fra Forsvarskommisjonen. Oppdraget er derfor gjort som en del av FFI-prosjektet «1619 – BAS: Totalforsvaret mot 2040».

Vi ønsker å takke Betina Slagnes, Tonje Grunnan, Torgeir Mørkved, Monica Endregard, Tormod Kalberg Sivertsen og Dagfinn Vatne for nyttige diskusjoner.

Kjeller, 15. november 2022
Julie Celine Bergaust
Frida Skjei
Stig Rune Sellevåg

1 Innledning

1.1 Bakgrunn

Det sikkerhetspolitiske utfordringsbildet for Norge har over lengre tid vært preget av stormaktsrivalisering samt en bredere og mer sammensatt virkemiddelbruk fra fremmedstatlige aktører. Russlands annektering av Krimhalvøya i 2014 var særlig med på å re-aktualisere bruken av begrepet «sammensatte trusler» i sammenheng med militærstrategiske utviklingstrekk. Russlands påfølgende invasjon av Ukraina 24. februar 2022 forverret utfordringsbildet ytterligere, og har medført store endringer i den sikkerhetspolitiske situasjonen i Europa. Den fremtidige utviklingen er usikker, og det er nødvendig å ta høyde for såkalte strategiske sjokk.[1]

Den 17. desember 2021 satte regjeringen ned en bredt sammensatt forsvarskommisjon. Kommisjonen har fått i oppdrag å vurdere «hvilke potensielle sikkerhets- og forsvarspolitiske veivalg og prioriteringer Norge kan ta for best å ivareta norsk sikkerhet i et 10–20-årsperspektiv». Kommisjonen skal legge frem sin utredning 3. mai 2023.

Regjeringen ønsker at Forsvarskommisjonen ser spesielt på følgende spørsmål (Forsvarskommisjonen, u.å.):

1. Hva betyr utviklingen i sikkerhetssituasjonen for hvilke sikkerhets- og forsvarspolitiske veivalg Norge står overfor på mellomlang og lang sikt?

2. Hvordan bør Forsvaret og forsvarssektoren på overordnet nivå videreutvikles og organiseres for å ivareta norske sikkerhetsinteresser?

3. Hva er sammenhengen mellom sammensatte trusler og andre sikkerhetspolitiske og militærstrategiske utviklingstrekk?

4. Hvordan kan forsvarssektoren best bidra til vern om Norges sikkerhet i lys av at utfordringsbildet treffer bredere, på flere samfunnsområder og berører stadig flere sektorer samtidig?

5. Hvilke muligheter og utfordringer representerer den teknologiske utviklingen for Norges sikkerhet og for utvikling av forsvarssektoren, herunder sektorens samhandling med sivile sektorer i rammen av totalforsvaret?

6. Hvordan vil bærekraftsmål, og klima og miljøendringer, påvirke forsvarssektoren og den sikkerhetspolitiske situasjonen i årene fremover?

[1] Strategiske sjokk er begivenheter som plutselig endrer vår strategiske situasjon og kjennetegnes ved at: (*i*) de har store konsekvenser, (*ii*) de utfordrer dagens oppfatninger så sterkt at det er vanskelig å overbevise andre om at hendelsen virkelig kan inntreffe og (*iii*) de er tilstrekkelig komplekse til at det er vanskelig å se for seg hvordan man kan håndtere dem (Freier, 2008 i Beadle, 2022).

7. Hvilke mekanismer, kapabiliteter og roller må prioriteres i forsvarssektoren for å bedre forstå, motvirke og forsvare nasjonale sikkerhetsinteresser mot et bredere utfordringsbilde og hva kan prioriteres ned for å gi rom for dette?

Som en del av kartleggingsarbeidet har Forsvarskommisjonen besluttet å bestille delutredninger hvor det hefter usikkerhet ved fremtidig utvikling, eller hvor det er behov for å få belyst konsekvenser og veivalg for forsvarssektoren grundigere. Denne rapporten er én av disse utredningene.

1.2 Oppdrag til Forsvarets forskningsinstitutt

Forsvarets forskningsinstitutt (FFI) har fått i oppdrag av Forsvarskommisjonen å belyse hvordan andre land håndterer sammensatte trusler. Finland, Sverige, Estland, Storbritannia, Nederland og Australia er aktuelle land for studien i henhold til oppdragsbeskrivelsen fra kommisjonen. Kommisjonen ønsker også at følgende spørsmål blir belyst for land hvor slik informasjon foreligger:

- Hvordan sammenstilles og deles informasjon for å etablere tverrsektoriell situasjonsforståelse og beslutningsgrunnlag?
- Hvilke tiltak har de utvalgte landene innført for å styrke nasjonens motstandsdyktighet mot sammensatte trusler?
- Hvordan samarbeider sivil og militær sektor når det gjelder å forebygge, avdekke og motvirke sammensatte trusler?

I tillegg ønsker Forsvarskommisjonen at delutredningen beskriver hva som er foreslått som beste praksis[2] for å styrke evnen til å forebygge, avdekke og motvirke sammensatte trusler. På bakgrunn av funnene på landnivå, og hva som er foreslått som mønsterpraksis, ønsker Forsvarskommisjonen å få belyst hva Norge kan lære av andre stater for å styrke evnen til å forebygge, avdekke og motvirke sammensatte trusler. Vi benytter terminologien «avskrekke», «avdekke» og «håndtere» i denne rapporten.[3]

Vi fremhever at det er andre lands tilnærminger og foreslått mønsterpraksis i Nato og EU som ligger til grunn for vurderingene av hva Norge kan lære. Rapporten har ikke vurdert norske myndigheters eller Forsvarets nåværende tilnærming. Vi overlater til Forsvarskommisjonen å vurdere om det er behov for å foreta noen sikkerhets- og forsvarspolitiske veivalg og prioriteringer for å bedre ivareta norsk sikkerhet i møtet med sammensatte trusler.

[2] Vi benytter begrepet «mønsterpraksis» som anbefalt av Språkrådet.
[3] Vi benytter begrepene avskrekke, avdekke og håndtere basert på oversettelse fra Monaghan *et al.* (2019).

1.3 Rapportens organisering

Denne rapporten er organisert på følgende måte: Vi beskriver begreper som brukes i rapporten i kapittel 2 og den metodiske tilnærmingen i kapittel 3 før vi presenterer foreslått mønsterpraksis i Nato og EU i kapittel 4. Der etter presenterer vi ulike staters forsvars- og sikkerhetsstruktur, identifiserte trusler og foreslåtte mottiltak i kapittel 5. I rapporten presenterer vi tilnærmingen til problematikken (gjennom ikke-uttømmende, men relevante eksempler) i Finland, Sverige, Estland, Storbritannia, Nederland og Australia. Til slutt diskuterer vi hva Norge kan lære av disse landene gjennom vurdering av tiltak i grupperingen avskrekke, avdekke og håndtering i kapittel 6, før vi gir anbefalinger i kapittel 7.

2 Begreper

FFI har lagt følgende begrepsbeskrivelser til grunn for oppdraget:

Statssikkerhet er å ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet (Meld. St. 5 (2020-2021), s. 11).

Nasjonal sikkerhet er beskrevet som «statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser (Meld. St. 5 (2020-2021), s. 11).

Nasjonale sikkerhetsinteresser er definert i sikkerhetsloven § 1-5 (Justis- og beredskapsdepartementet, 2019): Landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomisk stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner, og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil, eller bevisste handlinger (Meld. St. 5 (2020–2021), s. 11).

Totalforsvarskonseptet omhandler «gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i forbindelse med forebygging, beredskapsplanlegging, krisehåndtering og konsekvenshåndtering i hele krisespekteret fra fred via sikkerhetspolitisk krise til væpnet konflikt» (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2018; Meld. St. 5 (2020-2021), s. 11).

Sammensatte trusler og liknende begrep som «hybride trusler», «hybridkrig» og «gråsonekonflikt» er diskutert bredt i litteraturen. Det er uenighet om hvilket begrep som beskriver konseptet best, hvor bredt konseptet bør være, samt hvorvidt «sammensatte trusler» og liknende begrep bidrar til å skape mer forvirring og utydelighet enn konstruktiv klarhet (Se for eksempel Hoffman, 2009; Stoker & Whiteside, 2020; Wither, 2016). Det er ikke denne rapportens intensjon å gå inn i denne debatten, men å anerkjenne dens eksistens. Som rapporten vil vise benytter forskjellige stater seg av forskjellige begreper og forståelser av konseptet. I Norge ga Forsvarsdepartementet følgende definisjon i Meld. St. 10 ((2021–2022), s. 15):

> *Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske og finansielle, etterretningsmessige og juridiske*

virkemidler for å nå strategiske målsettinger. Virkemiddelbruken er gjerne distribuert bredt, er langsiktig i sin tilnærming og kombinerer åpne, fordekte og skjulte metoder.

Til denne rapportens formål bruker vi samme definisjon som Forsvarsdepartementet.[4] Vi har med andre ord begrenset denne rapporten til å omfatte virkemiddelbruk under terskel for væpnet konflikt. For å lese om lavintensivt hybridangrep på Norge i en fremtidig konflikt viser vi til Diesen (2018). Til tross for at vi bruker Forsvarsdepartementets definisjon i denne rapporten vil vi i vår gjengivelse av statenes tilnærming til sammensatte trusler oversette begrepet mest mulig direkte fra engelsk, og drøfte tiltakene slik de forskjellige landene presenterer dem selv.[5] Dette er for å fremheve forskjellene i ulike lands forståelse av konseptet. Vi gir en oversikt over hvordan andre sentrale begrep er oversatt i tabell 2.1.

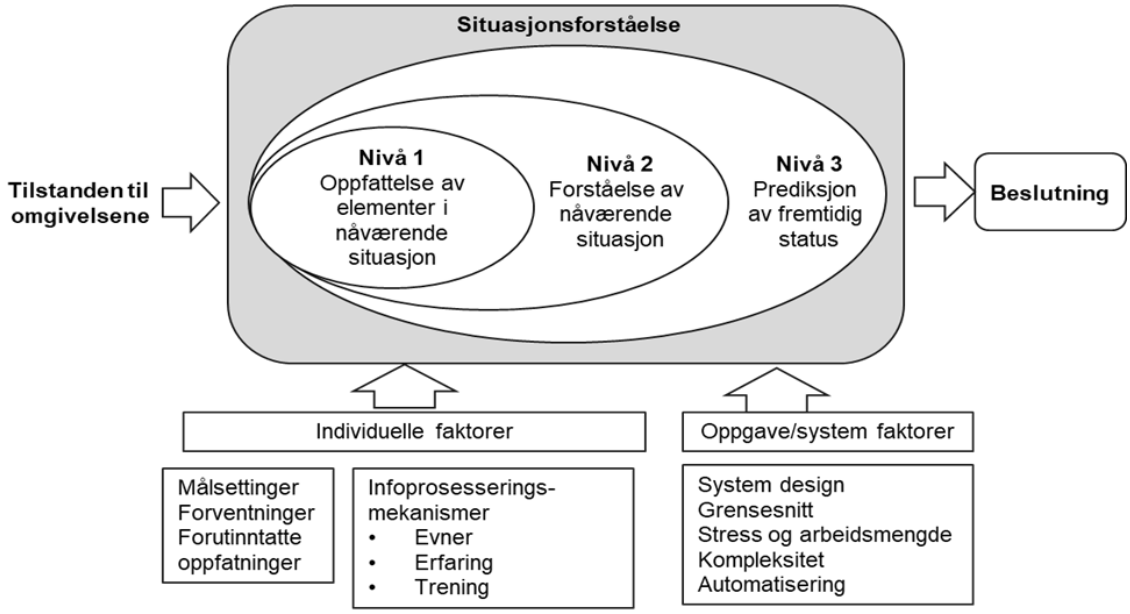
Tabell 2.1 Oversikt over oversettelse av sentrale begreper for denne rapportens formål.

Engelsk	**Norsk**
Mitigate	Begrense
Counter	Motvirke/mottiltak
Detect	Avdekke
Prevent	Forebygge
Deterrence	Avskrekke
Resilience	Motstandsdyktighet
Whole-of-society approach	Helhetlig samfunnstilnærming
Best practice	Mønsterpraksis

Situasjonsforståelse kan forklares ut fra modellen til Endsley (1995). En forenklet versjon av denne modellen er vist i Figur 2.1. Første nivå av situasjonsforståelse omhandler å oppfatte elementene i omgivelsene i nåværende situasjon. Dette krever informasjon om tilstanden til omgivelsene, for eksempel i form av et situasjonsbilde. Neste nivå av situasjonsforståelse er å forstå elementenes betydning i nåværende situasjon opp mot egne verdier, målsettinger og kontekst. Det tredje nivået omhandler prediksjon av elementenes fremtidige status. Det fattes en beslutning med utgangspunkt i de tre nivåene for situasjonsforståelse.

Evnen til å oppnå situasjonsforståelse er individuell, og avhenger av en rekke faktorer som evner, erfaring og trening. I tillegg påvirkes situasjonsforståelsen av en rekke andre faktorer, som forutinntatte meninger, forventninger, stress og hvordan informasjonen («situasjonsbildet») presenteres (Malerud *et al.*, 2021, s. 18). Ulike aktører vil således ha en situasjonsforståelse knyttet til egne oppgaver og funksjoner. I tillegg vil aktørene ha en situasjonsforståelse knyttet til felles oppgaver og funksjoner. Tilgang på rettidig og relevant informasjon om elementene i omgivelsene er derfor fundamentalt for å kunne oppnå god situasjonsforståelse. Det samme er kompetansen til beslutningstakerne, og til analytikerne som analyserer og sammenstiller informasjonen til et beslutningsgrunnlag.

[4] Denne definisjonen belager seg på en forståelse av at det er stater som benytter seg av sammensatte trusler, selv om stater også kan benytte seg av andre aktører (såkalte stedfortredere eller proxy-aktører).
[5] For eksempel omtaler vi det engelske begrepet «*hybrid warfare*» som «hybridkrig» på norsk.



Figur 2.1 Endsley (1995) sin modell for situasjonsforståelse (forenklet fremstilling etter Malerud et al. (2021, s. 18))

3 Metodisk tilnærming

Metoden som ligger til grunn i denne studien er todelt og innebærer litteratursammenstilling og tekstanalyse. Litteratursammenstillingen tar for seg akademisk litteratur på spørsmålet om mottiltak mot sammensatte trusler og relevante konsepter tilknyttet denne problemstillingen. Vi har tatt utgangspunkt i nøkkelordsøk i fagfellevurderte tidsskrift og «snøball»-effekten, der referanselisten i relevante artikler studeres med hensikt på å finne nye artikler av god kvalitet (Jalali & Wohlin, 2012; Webster & Watson, 2002). Rapporter fra sikkerhetspolitiske forskningsinstitutt og tankesmier har også blitt inkludert. I tillegg til faglitteraturen har vi supplert med kvalitativ tekstanalyse, herunder analyse av dokumenter. Tekstanalyse innebærer at tekst blir sett på som data en kan benytte til å skaffe informasjon om politikk (Benoit, 2020). Tekstene (korpuset) analysen består av er offisielle statlige strategier og policydokumenter vedrørende temaet sammensatte trusler. Det er nyttig å supplere den faglitteraturen med primærkildelesning for å unngå utvalgsskjevhet og at vi blir påvirket av funnene gjort i litteraturen (Thies, 2002). Rapporten har kun lagt ugradert informasjon til grunn for vurderingene som gjøres.

3.1 Forutsetninger

Det er en rekke forutsetninger som er lagt til grunn for denne studien. Det er andre lands tilnærminger og foreslått mønsterpraksis i Nato og EU som ligger til grunn for vurderingene av hva Norge kan lære. Rapporten har ikke vurdert norske myndigheters eller Forsvarets nåværende tilnærming, ei heller styrker og svakheter ved Norges tilnærming, utover overordnede betraktninger knyttet til norsk sikkerhetspolitikk og innretning av samfunnssikkerhetsarbeidet. Anbefalingene som rapporten gir, bør derfor ikke tolkes som at det er behov for å gjøre endringer i Norges nåværende tilnærming. Vi overlater til Forsvarskommisjonen å vurdere om det er behov for å foreta noen sikkerhets- og forsvarspolitiske veivalg og prioriteringer for å bedre ivareta norsk sikkerhet i møtet med sammensatte trusler.

Med dette som bakgrunn, legger vi to forutsetninger til grunn for studien:

- Foreslått mønsterpraksis er kunnskapsbasert
- De ulike landene har gjennomført en utredning om deres tiltak er hensiktsmessig for sin egen kontekst

Vi starter med å presentere foreslått mønsterpraksis i Nato og EU fordi vi dermed lettere kan identifisere relevante tiltak i landene vi studere og hva Norge kan lære av dette. Vi har ikke sammenfattet en uttømmende liste over tiltak som har blitt innført. Tiltak som nevnes er ikke gjensidig utelukkende. Med andre ord, at et tiltak blir nevnt i et land betyr ikke at det ikke har blitt introdusert i et annet.

3.2 Utvalg av land

For å finne relevant politikkutforming knyttet til sammensatte trusler er det aktuelt å velge land som er sammenlignbare med Norge. Vi undersøker politikkutformingen til Finland, Sverige, Estland, Nederland, Australia og Storbritannia. Disse statene ble foreslått i utlysningen, og vi har valgt å besvare direkte på forespørselen. Selv om landene i studien er like i form av å være vestlige land, er det relevant å identifisere forskjeller mellom dem (George & Bennett, 2005; Gerring, 2017). Vi gir her en kort oversikt over noen likheter og forskjeller mellom landene i studien. Først og fremst er den geografiske lokaliseringen en åpenbar forskjell, og geografi og nærhet til en identifisert trussel kan bidra til situasjonsforståelsen i befolkingen (Wijnja, 2022). Australia står både utenfor Nato, men også utenfor det europeiske kontinent. Finland og Sverige, som nylig har startet prosessen med å bli Nato-medlem, ligger geografisk som Norge og Estland i Nord-Europa og grenser til Russland. Norge, Sverige og Finland er også land med sterk styring og sterke institusjoner, lav korrupsjon samt relativt lav andel etniske minoriteter (Wither, 2020). Tillitsnivået blant de forskjellige landene er forskjellig. I 2009 svarte for eksempel 68 % av svenskene at «man kan stole på folk flest», mens bare 30 % av britene svarte det samme (Ortiz-Ospina & Roser, 2016). I 2021 var britenes tillit på 39,5 % ifølge OECD (2021b). I 2021 lå tilliten til myndighetene på 51,9 % i Estland og Australia, mens den i Nederland var på 58,5 %. Norge og Finland er de landene i studien som hvor befolkningen har høyest tillit til myndighetene (OECD, 2021b). Levestandarden i Australia, Sverige, Nederland og Finland er også spesielt høy ifølge den menneskelige utviklingsindeksen målt i 2021 (FN-sambandet, u.å.). Befolkningstettheten i Storbritannia og Nederland er betydelig høyere enn de andre landene (Roser et al., 2013). Storbritannia og Nederland har en annen kolonihistorie enn de øvrige landene (Jacobs, 2005).

3.3 Begrensninger

Studien har en rekke begrensinger. Det er for eksempel generelt utfordrende å finne samme informasjon for alle land når man gjennomfører sammenlignende studier (Gerring, 2017). På grunn av tidsbegrensinger har vi i denne studien ikke klart å skrive like utdypende på alle områdene som begrepet «sammensatte trusler» omfatter. Dette er følgelig en svakhet. Studien er derfor en begrenset gjennomgang av litteratur som har som formål å gi innblikk i ulike lands tilnærminger til sammensatte trusler.

Videre er det utenfor denne studiens rammer å gjøre egne undersøkelser om hvorvidt tiltakene fungerer i landene som denne studien omhandler. Dette vil kreve egne utredninger.

Det må også fremheves at i beskrivelsen av de ulike landenes tilnærming har vi tatt med beskrivelser av hendelser fra virkeligheten. Disse kan bli sett på som eksempler på hendelser som kan inngå i begrepet «sammensatte trusler». Vi vil likevel påpeke at disse hendelsene ikke nødvendigvis har vært en del av en sammensatt trusselstrategi. Eksemplene har blitt tatt med for å illustrere ulike typer aktiviteter og dens relevans, samt hvordan landene har svart på hendelsene.

4 Foreslått mønsterpraksis i Nato og EU

4.1 Nato

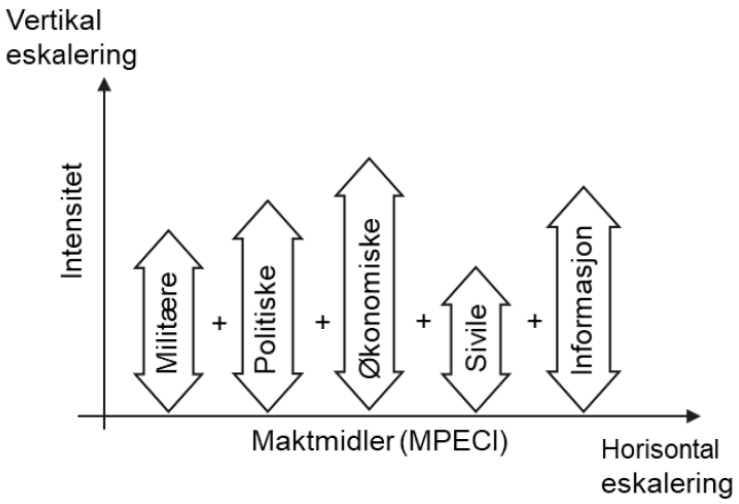
«Multinational Capability Development Campaign» (MCDC) er et USA-ledet initiativ i Nato som ble etablert i 2003 for å adressere flernasjonale kapabilitetsutfordringer. Arbeidet er organisert i kampanjer hvor interesserte nasjoner/institusjoner kan foreslå tema og melde seg på. Kampanjene har to års varighet og nasjoner/institusjoner kan være aktiv bidragsyter eller observatør. Hver kampanje skal resultere i et sluttprodukt (Malerud *et al.*, 2021).

MCDC-initiativet arbeidet i 2016–2017 med å øke forståelsen for hybridkrig. Arbeidet var todelt: Del 1 forsøkte å skape en felles beskrivelse av begrepet hybridkrig. Del 2 hadde som mål å skape et rammeverk for å hjelpe stater med å avskrekke, begrense og motvirke hybridkrig. Dette kapittelet beskriver arbeidsgruppens funn og forslag. MCDC-arbeidet endte med følgende beskrivelse av hybridkrig (Cullen & Reichborn-Kjennerud, 2017, s. 3):

> *Synkronisert bruk av flere maktmidler, skreddersydd for spesifikke svakheter på tvers av samfunnsfunksjoner, for å oppnå synergiske effekter.*

Selv om MCDC-arbeidet bruker begrepet «krig», beskriver MCDC-arbeidet hybridkrig som noe som forblir under åpenbar avdekking og under håndteringsterskel – med andre ord i fredstid. De fremhevet også hybridkrig som noe som utnytter kreativitet, usikkerhet, ikke-linearitet og kognitive elementer, samt holder seg utenfor åpenbar påvisning. Det analytiske rammeverket er tredelt: (*i*) kritiske funksjoner og sårbarheter, (*ii*) synkronisering av virkemidler og (*iii*) effekter og ikke-linearitet. Med kritiske funksjoner og sårbarheter menes aktiviteter og operasjoner på tvers av politiske, militære, økonomiske, sosiale, informasjonsrelaterte og infrastrukturrelaterte sektorer, som kan medføre forstyrrelser av tjenester som et system (for eksempel en stat) er avhengig av (Cullen & Reichborn-Kjennerud, 2017).

Synkronisering av virkemidler innebærer koordinering av maktinstrumenter i tid, sted og formål for å oppnå ønsket effekt. Karakteristisk for hybridkrig er synkronisert bruk av både militære og ikke-militære virkemidler. Synkroniseringen kan både eskalere horisontalt (antall virkemidler) og vertikalt (intensitet i virkemiddelbruk), som illustrert i figur 4.1 nedenfor. «Effekter» er forstått som endring av tilstanden til en enhet, men flere virkemidler med tverrsektorielle mål gjør at en lineær kjede av hendelser er vanskelig å identifisere. Eksempelvis kan et angrep på informasjonsdomenet få sin første effekt i det politiske domenet, men ikke eskalere til en krise før det samme angrepet får sin sekundæreffekt i infrastruktur (Cullen & Reichborn-Kjennerud, 2017, s. 14). Effekter trenger med andre ord ikke være direkte, ei heller oppstå i den samme sektoren som ble angrepet.



Figur 4.1 Synkronisert bruk av maktmidler i hybridkrig illustrert av MCDC-prosjektet. Figuren er en norsk oversettelse hentet fra Cullen og Reichborn-Kjennerud (2017, s. 9).

MCDC-prosjektet oppsummerte sine anbefalinger på følgende måte (Cullen & Reichborn-Kjennerud, 2017, s. 24–25):

- Hybridkrig er designet til å utnytte sårbarheter på tvers av politikk, militæret, økonomi, sosiale, informasjon og infrastruktur. Stater bør derfor gjennomføre sårbarhetsanalyser av kritiske funksjoner på tvers av alle sektorer og oppdatere analysene jevnlig.

- Nasjonale trusselvurderinger bør inkludere ikke-konvensjonelle kapabiliteter, slik som politiske, økonomiske, sivile og internasjonale verktøy. Disse analysene bør inkludere vurderinger av hvordan slike angrep kan være skapt som en synkronisert angrepspakke – skreddersydd for den spesifikke sårbarheten i målet.

- Nasjonal håndtering må være synkronisert og systematisk. Det bør etableres en funksjon som leder og koordinerer nasjonale tilnærminger til sårbarhet og trusselvurdering på tvers av sektorer.

- Hybridkrig er et internasjonalt problem og bør håndteres deretter. Stater bør koordinere en samlet tilnærming for å forstå, oppdage og besvare forsøk på hybridkrig. Multinasjonale rammeverk bør utvikles for å tilrettelegge for samarbeid på tvers av landegrenser, fortrinnsvis via eksisterende institusjoner og prosesser.

I 2019 kom del 2 av MCDC-arbeidet på hybridkrig, som fokuserte på hvordan en kan motvirke hybridkrig. Håndboken som ble utarbeidet hadde som hensikt å informere beslutningstakere og bidra med konseptuell forståelse. I dette arbeidet ble det gitt følgende anbefalinger (Monaghan *et al.*, 2019, s. 3–4):

- Sett realistiske strategiske mål.

- Identifiser passende terskler for håndtering. Respons kan være avhengig av aggresjonsnivået på handlingen, sårbarheten som potensielle tilsiktede handlinger kan forsøke å utnytte samt kapasitet for mottiltak.

- Design og implementer en strategi basert på de tre komponentene «avskrekke», «avdekke» og «respons».

- Utvikle institusjoner til å implementere de nevnte anbefalingene – på regjeringsnivå og gjennom multilateralt samarbeid – som er designet på en måte som gjør implementeringen egnet til formålet.

4.2 EU

I 2016 beskrev Europakommisjonen, gjennom Unionens høye representant for utenriks- og sikkerhetspolitikk[6] (heretter: Unionens høye representant), sammensatte trusler på følgende måte (Den Europeiske Union, 2016, s. 2):

> *Blandet bruk av tvang og undergravende aktiviteter, konvensjonelle og ukonvensjonelle metode (for eksempel diplomatiske, militære, økonomiske, teknologiske), som kan brukes på en koordinert måte av en statlig eller ikke-statelig aktør for å oppnå spesifikke mål, samtidig som en forblir under terskelen for formelt erklært krig*.

Ifølge Europakommisjonen bør hovedansvaret for å motvirke sammensatte trusler ligge hos medlemslandene, fordi de fleste nasjonale sårbarhetene er statsspesifikke. Likevel ser EU nytten av å ha koordinert håndtering på et EU-nivå gjennom EU-politikk og -verktøy for trusler som rammer nettverk og infrastrukturer på tvers av landegrenser. I tillegg anbefales det å forbedre samarbeidet mellom EU og Nato. De 22 foreslåtte handlingsforslagene setter søkelys på blant annet å øke oppmerksomhet, bygge motstandsdyktighet, forebygge, respondere på krise og gjenoppretting. I tillegg har det blitt fremmet sektorspesifikke handlingsforslag innen energi, transport og forsyningskjede, rom, forsvar, offentlig helse og matsikkerhet, cybersikkerhet, privat industri, finanssystemer, terrorfinansiering og samarbeid med naboregioner (Den Europeiske Union, 2016).

De overordnede handlingsforslagene var:

- Medlemsland inviteres til å gjennomføre en risikovurdering for å identifisere sårbarheter – inkludert indikatorer relatert til sammensatte trusler – som kan ramme nasjonale eller pan-europeiske strukturer og nettverk.

[6] På tidspunktet rapporten ble utgitt var det Federica Mogherini som var Unionens høye representant.

- Etableringen av en funksjon («EU Hybrid Fusion Cell») innad i den eksisterende «Intelligence and Situation Centre (EU INTCEN)»-strukturen i EU, som kan motta og analysere gradert og ugradert informasjon om sammensatte trusler. Medlemsland inviteres til å etablere egne nasjonale kontaktpunkt på sammensatte trusler for å sikre samarbeid og trygg kommunikasjon i EU Hybrid Fusion Cell.

- Unionens høye representant vil, sammen med medlemsland, utforske måter å oppdatere og koordinere kapasiteter til å levere proaktiv strategisk kommunikasjon, samt optimalisere bruk av mediaovervåking og språkspesialister.

- Medlemsland inviteres til å vurdere etableringen av et kompetansesenter (Centre of Excellence) for å motvirke sammensatte trusler («Hybrid CoE»).

- I samarbeid med medlemsland og interessenter vil Europakommisjonen identifisere felles verktøy og indikatorer med sikte på å forbedre beskyttelsen og motstandsdyktigheten til kritisk infrastruktur mot sammensatte trusler i relevante sektorer.

- Unionens høye representant vil, i samarbeid med medlemslandene, integrere, utnytte og koordinere kapabiliteter innen militær handlekraft for å motvirke sammensatte trusler innen EUs felles sikkerhets- og forsvarspolitikk.

- Unionens høye representant vil, i samarbeid med Europakommisjonen, fortsette den uformelle dialogen, samarbeidet og koordineringen med Nato. Dette omfatter situasjonsforståelse, strategisk kommunikasjon, cybersikkerhet og «kriseforebygging og respons» for å motvirke sammensatte trusler, samtidig som respekt for prinsippene om inklusivitet og autonomi i beslutningsprosessene innad i hver organisasjon ivaretas.

Wigell *et al.* (2021) utarbeidet en studie for Europaparlamentet med foreslått mønsterpraksis for en helhetlig samfunnstilnærming til å motvirke sammensatte trusler. Studien fremhevet behovet for å utvikle praksis for å motvirke sammensatte trusler som ikke går på bekostning av de verdiene en forsøker å beskytte. Det ble bemerket at noe fremgang hadde blitt gjort i EU, men at flere utfordringer gjenstår. For eksempel anerkjenner EU verdien av konseptet motstandsdyktighet, men det er fortsatt uklart hva slags konkret betydning og verdi det tilfører. Forpliktelser på toppnivå gjenspeiles heller ikke i planverk, og sammenhengen mellom nasjonal beredskap og sammensatte trusler samt helhetlig samfunnstilnærming bør tydeliggjøres. Det er også vanskelig å utvikle politikk når bruken av begrepet «sammensatte trusler» ikke skiller mellom forskjellige typer aktiviteter, intensitetsnivå på innblandingen og alvorlighetsgrad. Derfor foreslår Wigell *et al.* (2021, s. v) å skille mellom «hybrid innblanding», «hybride operasjoner» og «hybridkrig».

De fire overordnede anbefalingene var som følger (Wigell *et al.*, 2021, s. vi-viii):

1. *Introdusere felles vurderinger av sammensatte trusler*:

   - Etablere en felles begrepsforståelse innad i EU som bygger på den konseptuelle modellen utviklet av Hybrid CoE.
   - Jevnlig gjennomføring av trusselvurderinger av hele spekteret innen sammensatte trusler.
   - Starte en prosess for felles mottiltak for sammensatte trusler basert på trusselvurderingen.

2. *Skape en omfattende motstandsdyktighetstilnærming*:

   - Skape et miljø for et aktivt sivilsamfunn og uavhengig media.
   - Introdusere regulering og øke gjennomsiktigheten av sosiale medier.
   - Tildele tydelig roller og ansvar for å attributere sammensatte trusler og
   - Forebygge sammensatte trusler gjennom blant annet strategisk kommunikasjon og sanksjoner.

3. *Institusjonalisere en prosess med overvåking og måling av motstandsdyktighet:*

   - Identifisere sektorkrav til medlemslandene og EU-institusjonene.
   - Introdusere motstandsdyktighetsvurderinger gjennom modellering.

4. *Sette opp målinger for styrket sosial motstandsdyktighet*:

   - Øke bevissthet rundt samfunnets motstandsdyktighet i forbindelse med sammensatte trusler.
   - Promotere mediekunnskap i befolkningen.
   - Implementere programmer som har som mål å integrere diaspora og minoriteter
   - Utvikle lovgivning for å øke åpenhet ved valg.
   - Øke betydningen av motstandsdyktighet i forsynings- og verdikjeden i for eksempel forskning og utvikling, teknologi og handel.

4.3 Vurdering av foreslått mønsterpraksis

Det er nyttig at aktørene som benytter seg av begrepet «sammensatte trusler», eller liknende begreper, definerer begrepene de benytter. Dette er relevant for å forstå om aktørene setter begrepet i en kontekst for væpnet konflikt eller ikke. Det er også relevant for vurderingen av hvorvidt en kun ser på sammensatt virkemiddelbruk som aktiviteter som inngår i en synkronisert, forhåndsplanlagt kampanje, eller om opportunistiske aktiviteter også kan inngå i begrepsforståelsen. Styrken i begrepet ligger i forståelsen av hvordan fremmedstatlig innblanding kan utnytte sårbarheter på tvers av sektorer i samfunnet, og den nasjonale håndteringen bør derfor være systematisk og koordinert. *FFI er av oppfattelsen av at det er tydeligere å bruke begrepet sammen-*

satte trusler under terskelen for væpnet konflikt, og ikke begrepet «hybridkrig» fordi det kan bidra til forvirring. Et slikt syn støttes også av Wigell (2019), forskningsdirektør ved Finnish Institute of International Affairs (FIIA).

Unionens høye representant i EU fremhevet at hovedansvaret for å motvirke sammensatte trusler ligger hos medlemslandene (Den Europeiske Union, 2016). Selv om sårbarhetene er statsspesifikke, og det vil være nødvendig at hvert enkelt land håndterer hendelser som skjer innenfor egne landegrenser, vil ikke nødvendigvis effektene av hendelsene være begrenset til territoriet hvor hendelsene først har skjedd. Energiforsyning er et eksempel på hvordan nasjonale sårbarheter kan få effekter på tvers av landegrenser. Internasjonalt samarbeid som skaper situasjonsforståelse, slik MCDC-gruppen anbefaler, bør derfor bli sett i sammenheng med hendelseshåndteringen nasjonalt (Cullen & Reichborn-Kjennerud, 2017).

Det er også hensiktsmessig å identifisere nivåforskjeller mellom forskjellige aktiviteter, slik Wigell *et al.* (2021) anbefaler, for å kartlegge intensitet og alvorlighetsgrad. Å identifisere intensitet og alvorlighetsgrad vil kunne bidra til å identifisere terskler for håndtering, slik MCDC-gruppen har anbefalt, fordi det ikke nødvendigvis er hensiktsmessig å besvare alle enkeltaktiviteter som faller inn under sammensatte trusler. I vurderingen av håndtering skal det også med omhu vurderes hvordan håndtering, eller trussel om håndtering, kommuniseres som en del av en avskrekkingsstrategi (Monaghan *et al.*, 2019). Wigell *et al.* (2021) fremhever behovet for å ha verdiene en ønsker å beskytte tydelig definert før en utarbeider mottiltak. Dernest er det viktig at en ikke setter i gang tiltak som går på bekostning av rettsstatlige prinsipper og menneskerettigheter.

Avskrekking er trukket frem av MCDC-gruppen som foreslått mønsterpraksis for å forebygge og motvirke sammensatte trusler (Cullen & Reichborn-Kjennerud, 2017; Monaghan *et al.*, 2019; Sørensen & Nyemann, 2019). For å kunne vurdere om avskrekking er en egnet strategi for Norge, er det nødvendig å belyse om avskrekking av sammensatte trusler er en mulig og hensiktsmessig strategi. I det følgende vil vi derfor diskutere dette nærmere ut fra noen enkle betraktninger. Det henvises til Monaghan (2022) for en mer inngående diskusjon rundt dette spørsmålet.

Enkelt forklart kan en si at avskrekking handler om å påvirke motstanderens fiendtlige intensjoner gjennom trusler om at et angrep ikke vil lønne seg, fordi en motstanders sannsynlige kostnad vil overstige forventet gevinst (Morgan, 1977; Snyder, 1961). Dette krever en troverdig (klart kommunisert) evne (kapabilitet) og vilje (kredibilitet) til å hindre gevinst og/eller å påføre kostnader for angriperen (Jasper, 2015). Norge må med andre ord ta et aktivt valg om nasjonen har evnen og viljen til dette.

Vi vil ta utgangspunkt i en enkel operasjonsanalytisk tilnærming[7] basert på rapporten til Guttelvik & Hennum (2019) for å belyse spørsmålet om avskrekking av sammensatte trusler er mulig.

[7] Den operasjonsanalytiske tilnærmingen er en sterk forenkling, men benyttes som et pedagogisk hjelpemiddel for denne rapportens formål.

Under en forutsetning om at motstanderen gjør kost–nytte-vurderinger, kan en sette opp en enkel modell for å beskrive hvilke vurderinger motstanderen gjør før hen benytter sammensatte trusler for å oppnå sine målsettinger. For at en motstander skal gå til det skritt å gjennomføre slike handlinger, må motstanderen ha tro på at nytten av handlingen er større enn kostnader som kan følge fra eventuelle straffereaksjoner[8] dersom hen blir avslørt. Samtidig kan ikke motstanderen forvente at hen vil lykkes fullt ut med å oppnå sine målsettinger.

Forenklet operasjonsanalytisk tilnærming til avskrekking

Motstanderens forventede nytte av en tilsiktet handling kan beskrives som $U = p_{\text{gevinst}} U_{\text{gevinst}} - C$, hvor U er forventet nytte, U_{gevinst} er nytte dersom aktøren lykkes fullt ut, p_{gevinst} er sannsynligheten for at aktøren lykkes og C er kostnader som følge av straffereaksjoner (Guttelvik & Hennum, 2019).

Kostnader som Norge kan påføre en motstander kan beskrives som $C = C^{\text{Norge}} + p^{\text{allierte}} C^{\text{allierte}}$, hvor C^{Norge} er Norges egen evne til å gjennomføre straffereaksjoner, C^{allierte} er alliertes straffereaksjoner og p^{allierte} er sannsynligheten for å få alliert støtte (Guttelvik og Hennum, 2019).

Absolutt avskrekking innebærer at forventet nytte er mindre eller lik null ($U \leq 0$). Begrenset avskrekking innebærer at forventet nytte er mindre enn et gitt terskelnivå ($U < T$).

Avskrekking ved nektelse innebærer at p_{gevinst} reduseres.
Avskrekking ved straff innebærer at $C \geq p_{\text{gevinst}} U_{\text{gevinst}}$.

For å oppnå absolutt avskrekking må forventet nytte av handlingen være mindre eller lik kostnadene som følger fra forventede straffereaksjoner. Under terskelen for direkte væpnet konflikt vil absolutt avskrekking av sammensatte trusler verken være mulig eller ønskelig i et vestlig demokratisk samfunn. Det er også usannsynlig at revisjonistiske stormakter som Russland og Kina sin bruk av sammensatte trusler kan avskrekkes fullstendig. Det er derfor mer hensiktsmessig å betrakte strategier hvor målet er å oppnå at motstanderens handlinger ikke medfører uakseptabel risiko, slik MCDC-gruppen foreslår.

For at begrenset avskrekking av sammensatte trusler skal kunne oppnås,[9] må avskrekkingen enten redusere sannsynligheten for at motstanderen lykkes i tilstrekkelig grad (hindre gevinst) eller påføre motstanderen store nok kostnader. Førstnevnte strategi kan karakteriseres som *avskrekking ved nektelse*.[10] For at denne formen for avskrekking skal virke mot sammensatte trusler, må forsvareren ha en troverdig evne til å hindre motstanderen i å oppnå sine målsettinger. Viktige

[8] Med straffereaksjoner mener vi her mottiltak ved hendelseshåndtering basert på avskrekkingsteori og ikke straff begrenset til kun strafferettslig forfølgelse.
[9] Med bakgrunn i den operasjonsanalytiske tilnærmingen, forutsettes her at U_{gevinst} ikke kan påvirkes.
[10] Omtalt som «*deterrence by denial*»

elementer her vil være å opprettholde motstandsdyktighet i samfunnet, opprettholde tillit mellom myndighetene og befolkningen, og ha troverdig evne til krisehåndtering, jf. MCDC-gruppens foreslått mønsterpraksis (kapittel 4.1).

Sistnevnte strategi kan karakteriseres som *avskrekking ved straff*.[11] For at denne formen for avskrekking skal virke, må forsvareren ha troverdig evne til (*i*) å oppdage sammensatte trusler, (*ii*) å attribuere handlingene til riktig aktør og (*iii*) å gjennomføre tilstrekkelige straffereaksjoner mot motstanderen. For småstater som Norge vil det videre være en fordel å inngå allianser med stormakter for å øke evnen til å gjennomføre straffereaksjoner.

Skal så strategier for begrenset avskrekking av sammensatte trusler baseres på nektelse eller straff? Ut fra erfaring med faktiske hendelser som datanettverksoperasjoner, uønsket valgpåvirkning og bruk av migranter, er det usannsynlig at avskrekking ved nektelse alene vil være en tilstrekkelig troverdig strategi selv for begrenset avskrekking. Det er fordi det i realiteten ikke vil fungere i et åpent og demokratisk samfunn. Det er rett og slett ikke ønskelig å lukke samfunnet i så stor grad at avskrekking ved nektelse er oppnådd. Så lenge slike sammensatte trusler ikke avskrekkes med troverdige straffereaksjoner, er det grunn til å forvente at en motstander vil fortsette å benytte slike handlinger.

Betyr dette at straff er mest egnet form for avskrekking mot sammensatte trusler? Som nevnt, krever avskrekking ved straff at en har troverdig evne til å oppdage, attribuere og straffeforfølge sammensatte trusler. I takt med den økende betydningen av digital teknologi i samfunnet har debatten knyttet til *cyberavskrekking*, og hvorvidt det er mulig å avskrekke angrep i det digitale rom, blitt aktualisert (Gjesvik & Øverbø, 2019). Sikkerhetssituasjonen i cyberdomenet påvirkes av et nærmest ubegrenset antall aktører, noe som i hovedsak stammer fra at tilgangen til og antallet *angrepsvektorer*[12] i domenet, er enormt. Ifølge Jasper (2015, s. 78 i Kristiansen & Hoem, 2019) muliggjør angrepsvektorene og kompleksiteten disse representerer en rekke handlinger som er vanskelig å oppdage og beskytte seg mot i det digitale rom. Satt på spissen kan hvem som helst med tilgang til internett påvirke sikkerhetssituasjonen, samtidig som omfanget av mulige sikkerhetstrusler gjør det krevende å beskytte seg mot alle trusler og reagere på det en anser som overtramp (Kristiansen & Hoem, 2019, s. 256). Denne uoversiktlige situasjonen, kombinert med at det mulig å skjule angrepets opprinnelse, og dermed angriperens identitet, utfordrer evnen til å attribuere digitale angrep (Rid & Buchanan, 2015).

Selv om enkelte hevder at problemet med attribusjon av datanettverksoperasjoner er løst (Alperovitch, 2018), er det tid- og ressurskrevende. Det er også behov for mer kunnskap om når en skal gå til offentlig attribusjon og hva håndteringen skal innebære (Egloff, 2020; Egloff & Smeets, 2021). Per 2019 fantes det ifølge Kristiansen og Hoem (2019) ingen tydelige og internasjonalt anerkjente retningslinjer for hvordan en best forvalter proporsjonalitetsprinsippet i cyberdomenet. Mangel på slike retningslinjer gjør følgelig håndtering vanskeligere. Som Etterretningstjenesten (2022, s. 19) påpeker, har aktører fortsatt med «synlige og støyende operasjoner som

[11] Omtalt som «*deterrence by punishment*»
[12] «[...] *a specific method or technique to access equipment, computers, or systems to deliver a hostile payload for a malicious outcome*» (Jasper, 2015, s. 6).

er enkle å oppdage» til tross for at myndigheter i Norge og andre land har gått ut offentlig og sagt hvem det er som står bak. Dessuten er datanettverksoperasjoner bare ett av mange virkemidler en aktør kan benytte. Ser vi på uønsket påvirkningsaktivitet, er det også et spørsmål om hvor langt myndigheter kan gå i avskrekking gjennom straff av fremmedstatlige forsøk på påvirkning av politiske beslutningsprosesser og det offentlige ordskiftet, uten at det setter begrensninger på ytringsfriheten.

Ut fra disse enkle argumentene synes det åpenbart at avskrekking mot sammensatte trusler ikke kan baseres på enten nektelse eller straff, men begge former for avskrekking må være tilstede for å være en troverdig strategi. Flere studier peker også på dette (Kersanskas, 2020; Monaghan, 2022; Monaghan et al., 2019; Nye, 2017; Takahashi, 2018; Wigell, 2021).

Wigell (2021) har nylig foreslått en slik tospors avskrekkingsstrategi som på engelsk er omtalt som *«democratic deterrence»*. I denne strategien utnyttes både avskrekking ved nektelse og avskrekking ved straff. I motsetning til tradisjonell avskrekkingsteori, baseres *avskrekking gjennom demokrati* på samfunnets samlede ressurser, bruk av myk makt og ikke-militære virkemidler for å oppnå begrenset avskrekking. Wigell (2021) fremhever også at demokratiske normer og verdier er strategiske instrumenter som kan benyttes for å avskrekke autoritære regimer. Følgelig kan responsen til vestlige demokratier være asymmetrisk fordi symmetrisk respons vil føre til ytterligere undergraving av liberale og demokratiske verdier (Wigell, 2021). Styrking av demokratiske verdier og prosesser er derfor viktige elementer for å oppnå avskrekking ved nektelse. Liknende argumenter fremføres også av Rácz (2015, s. 92) som forsvar mot sammensatte trusler:

> *[G]ood governance needs to be interpreted in the broad sense. In addition to a democratic political structure and wellfunctioning public administration, it includes respect for human rights, transparency, media freedom, the rule of law and proper rights guaranteed to ethnic, national, religious and other minorities, all in order to improve the domestic democratic legitimacy and support of the government, and hence the very stability of the state.*

Avskrekking ved nektelse må derfor være en langsiktig strategi som har bred politisk forankring. Bred politisk forankring over tid vil potensielt være problematisk å oppnå fordi hvert regjeringsskifte vil medføre endringer i politikk knyttet til områder som helse, velferd, finans, industri, energi, transport, forsyningskjeder, rom, forsvar, matsikkerhet, medier, innvandring, kriminalitet, og så videre. Selv om hovedtrekkene i forsvars- og sikkerhetspolitikken kan ligge fast ved ulike regjeringer, kan andre politikkområder direkte eller indirekte påvirke samfunnets motstandsdyktighet mot sammensatte trusler.

Motstandsdyktighet innbefatter ikke bare motstandsdyktighet i kritisk infrastruktur og samfunnsfunksjoner, men også i forsyningskjeder, i lokalsamfunnet og på individnivå (Wigell *et al.*, 2021). Samtidig påpeker Monaghan *et al.* (2019) at styrking av samfunnets motstandsdyktighet trolig ikke vil føre til endring i adferd blant fremmedstatlige aktører som benytter sammensatte trusler. Likevel fremhever flere studier at god motstandsdyktighet i samfunnet som viktig for å

oppnå avskrekking ved nektelse (Kersanskas, 2020; Monaghan, 2022; Monaghan *et al.*, 2019; Wigell, 2021). Som Kersanskas (2020, s. 11) påpeker:

> *To deter by denial means to show the hostile actor that one can easily absorb the attack with minimal costs to the state that is the target of the hybrid activity.*

Til tross for at motstandsdyktighet i samfunnet ikke endrer adferden til andre stater kan det med andre ord potensielt påvirke i hvilken grad bruk av sammensatte trusler har en effekt.

Når det kommer til avskrekking ved straff, foreslår Wigell (2021) at dette blant annet kan gjøres ved å fremme demokrati og menneskerettigheter i autoritære regimer. En fare med en slik strategi er at det kan føre til press og represalier mot demokratiske krefter i slike regimer. En avskrekking som regimet oppfatter som en eksistensiell trussel kan derfor føre til uønsket eskalering (Pezard & Rhoades, 2020). Avskrekking ved straff må derfor være aktør-spesifikk og riktig kalibrert (Kersanskas, 2020, s. 14). Monaghan *et al.* (2019, s. 44) karakteriserer derfor avskrekking mot sammensatte trusler på følgende måte:

> *Hybrid deterrence is ultimately about marginal gains through tailored deterrence. […] a logical, actor-centric approach that disaggregates the concept of hybrid warfare and considers marginal gains has potentially vast utility.*

Betydningen av å forstå den andre statens sikkerhetspolitikk og strategiske kultur for å skreddersy en effektiv avskrekkingsstrategi fremheves også av Gjesvik og Øverbø (2019) i konteksten av å avskrekke cyberangrep. I tillegg må evnen til troverdig militær avskrekking opprettholdes for å minimere risikoen for uønsket eskalering til væpnet konflikt (Monaghan et al., 2019; Wigell, 2021). Implementering av avskrekkingsstrategier mot sammensatte trusler bør derfor inngå som en del av et helhetlig nasjonalt forsvars- og sikkerhetskonsept (Balcaen et al., 2021). Ved vurdering av Forsvarets rolle i arbeidet med å motvirke sammensatte trusler fremstår evne til troverdig militær avskrekking og evne til å oppnå situasjonsforståelse gjennom blant annet etterretning, som sentralt.

5 Ulike lands tilnærminger

5.1 Finland

Finland har, i likhet med Norge og Sverige, et forsvarskonsept som belager seg på sivil-militært samarbeid. Dette går under navnet «*Comprehensive Security Concept*». Samarbeidet gjelder ikke bare militære og offentlige institusjoner, men også på tvers av statlige myndigheter, og inkluderer privat sektor, frivillige organisasjoner og privatpersoner for å sikre kritiske samfunnsfunksjoner. I tillegg bidrar regionale myndigheter, akademia og forskning inn i sikkerhetskonseptet. På et institusjonelt nivå er det statsministerens kontor som har ansvar for situasjonsforståelse og samhandlingskoordinering (Ferm *et al.*, 2018; Wigell *et al.*, 2021). For en oversikt over totalforsvarsaktørers roller og ansvar i Finland, viser vi til Wigell *et al.* (2022).

Etter den kalde krigens slutt har Finland, i motsetning til Norge og Sverige, beholdt mer av «invasjonsforsvaret». Finland står derfor relativt sett mer klar til mobilisering av samfunnet enn sine naboer. Eksempler på hvordan Finland har videreutviklet sikkerhetskonseptet siden 1990-tallet er lagring av mat, drivstoff og utstyr for sivilt forsvar. Sikkerhetskonseptet skal bidra til informasjonsdeling, felles målsetting og forpliktelse til samarbeid. Dette skal bidra til fleksibel koordinering av aktiviteter. I tillegg er det et mål å øke kostnaden med fiendtlig aggresjon og senke mulighetene for suksess (Wigell *et al.*, 2021; Wither, 2020). Finlands søknad om Nato-medlemskap vil også kunne bidra til dette.

I sin definisjon av sammensatte trusler beskriver den finske regjeringen sammensatt påvirkning («hybrid influencing») som bruk av flere militære virkemidler samtidig, også i kombinasjon med andre virkemidler, for eksempel økonomiske eller teknologiske verktøy, i tillegg til informasjonsoperasjoner og sosiale medier. Sammensatt påvirkning presiseres som noe som spesifikt forsøker å påvirke en stats akilleshæl for å oppnå egne mål (Regjeringen (Finland), 2016, s. 13). I Finland er psykologisk motstandsdyktighet spesielt vektlagt (Wither, 2020).

For å håndtere sammensatte trusler har Finland satt i gang en rekke tiltak gjennom sitt sikkerhetskonsept. Disse tiltakene er i stor grad tilknyttet opplæring og situasjonsforståelse. I 2014 gjennomførte den finske sikkerhetskomiteen en undersøkelse om sammensatte trusler. I undersøkelsen ble både kjente og mulige fiendtlige handlinger kartlagt, samt evaluert opp mot mulige svakheter innenfor diplomati, informasjon, militæret og økonomi. Resultatene fra undersøkelsen ble diskutert i møter mellom utenriks- og sikkerhetspolitisk ministerkomité (Ministerial Committee on Foreign and Security Policy) og den finske presidenten. En oppfølgingsrapport ble publisert i 2017. Det ble konkludert med at tiltaket bidro til bedre forståelse for beredskapsnivået blant administrasjonen og at forbedringspotensialet til kapabilitetene ble belyst (Ferm *et al.*, 2018).

Det er tilknyttet en rekke opplærings- og utdanningsprogram til det finske sikkerhetskonseptet. Dette inkluderer blant annet nasjonale kurs ved den finske forsvarshøgskolen, bordøvelser for politisk ledelse, tverrsektorielle øvelser hvert fjerde år (VALHA) og integrering av problemstil-

linger tilknyttet sammensatte trusler i pensum på universitetsnivå. Det har også blitt gjennomført opplæringsaktiviteter i privat sektor og initiativ for å øke befolkningens medieforståelse. Å sikre et fritt, mangfoldig og ansvarlig media har blitt fremhevet som en essensiell del av sikkerhetskonseptet (Ferm *et al.*, 2018; Wigell *et al.*, 2021).

I den finske regjeringens situasjonssenter har det blitt opprettet en gruppe for analyse av sammensatte trusler. Dette nettverket er satt sammen av representanter fra alle departementer samt akademia og privat sektor. De jobber i hovedsak med ugradert informasjon, men omlag halvparten av medlemmene i nettverket har sikkerhetsklarering og kan bidra til analyse av gradert materiale (Ferm *et al.*, 2018). I tillegg ligger det internasjonale kompetansesenteret (Centre of Excellence) for å motvirke sammensatte trusler («Hybrid CoE»), som EU anbefalte å opprette, i Helsingfors.

Det har blitt gjennomført og foreslått en rekke nye lover for å motvirke sammensatte trusler i Finland. I 2017 ble det foreslått en lovendring for å styrke territoriell overvåking. Forslaget omfattet oppkjøp av land og eiendom, samt status for personer med dobbelt statsborgerskap (Ferm *et al.*, 2018). Disse lovforslagene kan bli sett i lys av reelle utfordringer Finland stod overfor på dette tidspunktet. I 2018 ble det for eksempel avdekket at en russisk oligark ved navnet Pavel Melnikov hadde bygget et større anlegg med høyt militært nivå i et område av større strategisk betydning i Finland (Ellehuus, 2020; Higgins, 2018).

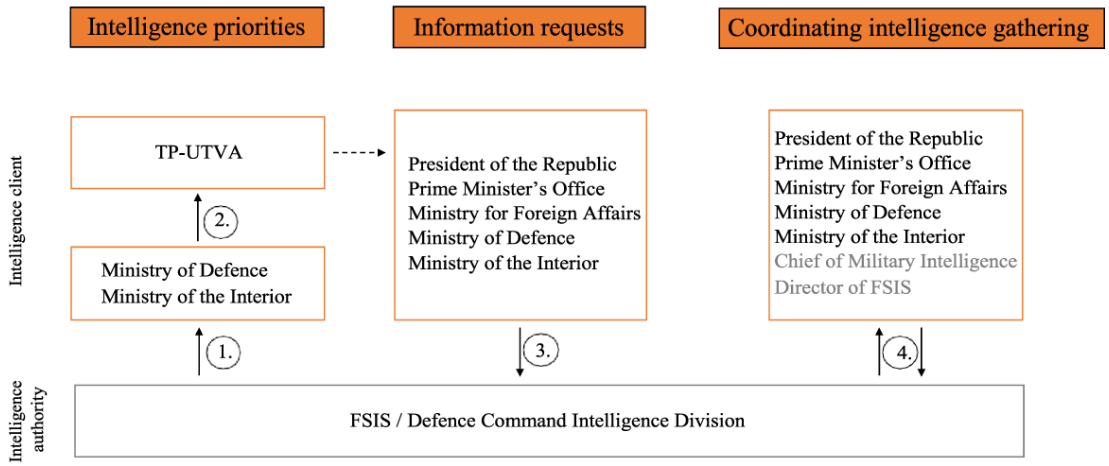
Aksjonen mot den russiske oligarkens finske øy (2018)

Den 22. september 2018 gjennomførte finsk politi og forsvar en aksjon på den finske øya Sakkiluoto, eid av den russiske oligarken Pavel Melnikov. På øya hadde Melnikov bygget opp ni kaier, en helipad, et kamuflert basseng og nok utstyr til å huse en liten hær. I tillegg var øya utstyrt med avansert informasjons- og overvåkingsteknologi. Sakkiluoto, som ligger mellom Østersjøen og Bottenviken, er strategisk plassert i nærheten av petroleumsraffineriet Naantali og havnen Turku. Turku, og de nærgående sjøveiene, huser rundt 90 prosent av finsk eksport og import (Ellehuus, 2020). Plasseringen bidro til spekulasjoner om at Russland var i ferd med å planlegge en hybridkrigkampanje mot Finland. Russiske myndigheter har avslått dette og finske myndigheter uttalte at bakgrunnen for aksjonen var å bekjempe hvitvasking og skatteunndragelser. Sakkiluoto var en av 17 steder som ble aksjonert mot samme dag av mer enn 400 innsatspersonell (Ellehuus, 2020; Higgins, 2018).

Finland har også innført lovgivning som tillater samarbeid mellom de sivile sikkerhetsmyndighetene (Finnish Security and Intelligence Service, FSIS) og den militære etterretningen (Finnish Defence Intelligence Agency, FDIA). Som figur 5.1 nedenfor viser, går ikke informasjonsutvekslingen bare mellom FSIS og FDIA, men også andre offentlige myndigheter og internasjonale partnere kan motta informasjon (Lohse, 2020a, 2020c). Informasjonen kan likevel ikke bli ukritisk delt. Det foreligger for eksempel krav om at flere kriterier må vurderes før informa-

sjonsutveksling som omhandler personopplysninger kan finne sted internasjonalt: Menneskerettighetssituasjonen og standard for informasjonsbeskyttelse i landet som mottar personopplysninger, internasjonale avtaler, betydningen av å dele informasjon for Finland i internasjonalt samarbeid og betydningen av å dele informasjonen for rettighetene til personen det angår (Lohse, 2020c, s. 284–285). Endringen i lovgivning har bidratt til at Finland ikke lenger har separat innenlands- og utenlandsetterretning, men heller en sivil og en militær etterretning. Det er innenriksdepartementet som gir prioriteringer på hvilke temaer den sivile etterretningen skal innhente informasjon og rapportere på. Prioriteringene kan endres gjennom året ved behov (Innenriksdepartementet (Finland), u.å.). Resultatet har ifølge den finske regjeringen vært at den nasjonale sikkerhetssituasjonen har blitt forbedret (Regjeringen (Finland), 2021).

Andre tiltak Finland har innført er opprettelsen av en såkalt «Hybrid-Ambassadør». Ansvaret som er tillagt rollen er å bygge profil for problemstillinger tilknyttet sammensatte trusler internasjonalt og å styrke internasjonalt samarbeid (Ferm *et al.*, 2018). I tillegg blir nordisk samarbeid for å forbedre motstandsdyktighet og totalforsvar anbefalt av både Joakim Møller ved Institutt for forsvarsstudier (IFS) og den tidligere finske diplomaten Pauli Järvenpää (Järvenpää 2017, s. 14 og Møller, 2019, s. 251 i Wither, 2020).



Figur 5.1 Styring og koordinering av etterretning i Finland (Lohse, 2020b, s. 72). Lisens: CC BY 4.0.

5.2 Sverige

Den svenske totalforsvarsmodellen defineres som militære og ikke-militære aktiviteter som forbereder samfunnet på krig. Den svenske nasjonalforsamlingen, regjeringen, offisielle myndigheter, private bedrifter, frivillige organisasjoner og individer regnes som en del av totalforsvaret (Forsvarskommisjonen (Sverige), 2017). Etter den kalde krigens slutt valgte imidlertid Sverige – i motsetning til Finland – å bygge ned sitt totalforsvar. Å forberede seg på væpnet konflikt ble regelrett sett på som unødvendig og dyrt (Lindgren & Ödlund, 2017). Nedbyggingen innebar

store kutt i forsvarssektoren og fokus lå ikke lenger på territorielt forsvar. Det var ikke før i 2015 at regjeringen etterspurte et nytt totalforsvarskonsept (Forsvarskommisjonen (Sverige), 2017, 2019). Tanken bak det nye totalforsvarskonseptet er at det ikke bare skal fungere under krig, men bidra til å forhindre og håndtere store kriser. Motstandsdyktighet, Natos syv grunnleggende forventninger og avskrekking blir lagt til grunn (Forsvarskommisjonen (Sverige), 2019; Roepke & Thankey, 2019; von Sydow, 2018; Wigell *et al.*, 2021). For en oversikt over totalforsvarsaktørers roller og ansvar i Sverige, viser vi til (Wigell *et al.*, 2022).

Remilitarisering av Gotland (2015)

Den svenske øya Gotland, som ligger i Østersjøen midt mellom Sverige og Baltikum, ble i 2004 i stor grad demilitarisert. Øya, som er Sveriges største, har i underkant av 60 000 innbyggere og den eneste byen Visby, står på UNESCOs verdensarvliste. Oberst Mattias Ardin (51), som er sjefen for regimentet fortalte til Forsvarets Forum at «Russernes ulovlige annektering av Krim i 2014 er nøkkelen til oppbyggingen av hæren her på Gotland» (Skjævesland, 2020). Etter den påfølgende russiske invasjonen i Ukraina i 2022 har svenske myndigheter sett et behov for å bygge opp igjen de militære styrkene på øya. I 2015 bestemte den tverrpolitiske Försvarsberedningen at forsvaret skulle returnere, og i 2018 var det utplassert flere militære enheter og drøyt 300 personer (Skjævesland, 2020). Den militære tilstedeværelsen økte i januar 2022 på grunn av observasjoner av flere russiske krigsskip i Østersjøen (Karlsen, 2022). Den svenske forsvarsministeren, Peter Hultqvist, blir sitert av Norges Forsvarsforening på at den geografiske plasseringen av øya er av betydning, og at «den som behersker Gotland, behersker hele Østersjøen». I tillegg uttalte forsvarsministeren bekymring for at øya skulle bli utsatt for «hybride operasjoner», med hensikt å skape frykt (Hjorth, 2022). 30 000 mennesker har meldt seg til tjeneste i heimevernet i Sverige siden krigen i Ukraina begynte (Karlsen, 2022).

Å bygge ut infrastruktur og motstandsdyktighet i et totalforsvarsperspektiv forblir imidlertid et langtidsprosjekt for Sverige (Wither, 2020). Den svenske forsvarskommisjonen rapporterte i 2017 om de store utfordringene knyttet til å revitalisere et totalforsvarskonsept i et samfunn og en økonomi som hadde forandret seg mye siden 1980-tallet (Forsvarskommisjonen (Sverige), 2017). Ved Totalforsvarets forskningsinstitutt i Sverige (FOI) har forskere anbefalt at dagens konsept, som er karakterisert som en reaktiv, hendelsesdrevet tilnærming til kriseledelse, bør erstattes av strategisk sivil forsvarsplanlegging for å adressere forskjellige scenarioer (Lindgren & Ödlund, 2017). Den svenske forsvarskommisjonen anerkjente også at et totalforsvarskonsept som belager seg på befolkningens bidrag også er avhengig av befolkningens forsvarsvilje, både i fredstid og krigstid.[13] Derfor ble det satt ned en gruppe for å utrede mulighetene innen psykologisk forsvar mot propaganda og desinformasjon, samt sendt ut informasjonssedler til alle husholdninger (MSB, 2018; Wither, 2020).

[13] Det gjennomføres et PhD-prosjekt om norsk forsvarsvilje i et totalforsvarsperspektiv ved FFI i perioden 2021–2025.

Nødvendig håndtering i krisetider kan forsinkes av at den svenske regjeringen mottar sitt mandat til handling fra sin nasjonalforsamling. Det er spesielt vanskelig å koordinere den ikke-militære siden av totalforsvaret, fordi det er mange forskjellige aktører. Håndteringen av koronapandemien har utløst spørsmål om hvorvidt dagens system for å besvare gråsonetrusler er raskt nok (Wigell et al., 2021). Forsvarskommisjonens leder, Björn von Sydow, har likevel fremhevet at det blir stadig viktigere å aktivt beskytte det åpne samfunnet, suverenitet og rettsstatsprinsipper (von Sydow, 2018). I den forbindelse bør det fremheves at Sverige har gjort endringer i sin etterretning som førte til at Sverige ble dømt i Den europeiske menneskerettighetsdomstolen (EMD) i Strasbourg i 2021. Sverige ble dømt for brudd på retten til privatliv i saken *Centrum for Rättvisa v. Sverige.* Bakgrunnen for saken var Sveriges bulkinnsamlingssystem for etterretningsformål, hvor det spesielt ble påpekt at det svenske systemet blant annet manglet regelverk for sletting av data og en uavhengig etterkontroll (Grand Chamber ECtHR, 2021b; NIM, 2021).

Den svenske forsvarskommisjonen fremhevet også utfordringene knyttet til totalforsvarsorganisering, psykologisk forsvar, elektronisk kommunikasjon og cybersikkerhet, beskyttelse av sivilbefolkningen, rettshåndhevelse, helse og finansberedskap (Forsvarskommisjonen (Sverige), 2017, 2019). Tilgang på matvarer og andre tjenester har blitt fremhevet som viktig å opprettholde under en potensiell krise (Forsvarskommisjonen (Sverige), 2017; von Sydow, 2018). Utfordringene skissert av forsvarskommisjonen reflekteres i Sveriges sikkerhetsstrategi for 2016–2020, der det spesielt ble fremhevet et behov for koordinering og planlegging i sivilt forsvar, sivilt bidrag til forsvarsevne og psykologisk forsvar mot desinformasjon. Myndigheten för samhällsskydd och beredskap (MSB), tilsvarende Direktoratet for samfunnssikkerhet og beredskap (DSB) i Norge, ble gitt en sentral rolle (Gotkowska, 2021; Wigell *et al.*, 2021).

Beredskap og sivil-militært samarbeid har blitt viktigere ettersom både statlige og ikke-statlige aktører har funnet nye måter å påvirke samfunnet som ikke belager seg på tradisjonell militærmakt. En rapport fra Totalförsvarets forskningsinstitut (FOI) påpeker at sivil beredskap og samfunnet forøvrig må kunne motvirke denne type gråsoneaktiviteter (Jonsson *et al.*, 2019). Forsvarskommisjonen anbefalte at politistyrker må benyttes for å beskytte kritisk infrastruktur og andre kritiske funksjoner under forhøyet beredskap, krig eller hybride situasjoner. Politiet hadde imidlertid ikke slike ressurser tilgjengelige i 2017, og foreslo derfor å øke antall personell i politiet med 3000 innen 2025 (Forsvarskommisjonen (Sverige), 2017).

Et forslag til ny totalforsvarslovgivning fra 2020 fremhevet rollen til de ikke-militære myndighetene, offentlig-privat samarbeid og behovet for regional samarbeid i med de nordiske landene, samt Storbritannia og USA (Regjeringen (Sverige), 2020). Regionalt samarbeid, spesielt med Finland og Norge, ble også anbefalt av den svenske Forsvarskommisjonen (Forsvarskommisjonen (Sverige), 2017, 2019). Forslaget til ny totalforsvarslovgivning kom før Sverige søkte medlemskap til Nato og Riksdagsvalet (Stortingsvalget) i 2022, men den svenske forsvarskommisjonen har fått i oppdrag å levere sin siste anbefaling for forsvarsperioden 2026–2030 i 2025 (Regjeringen (Sverige), 2020). Det er derfor forventet oppdateringer rundt dette teamet.

Sverige utnevnte i 2018 en ambassadør og spesialutsending i utenriksdepartementet for å motvirke sammensatte trusler. Dette har vært et tiltak for å bidra til økt internasjonalt samarbeid for å motvirke desinformasjon. I 2019 påpekte den første hybrid-ambassadøren, Fredrik Löjdquist,

at de byråkratiske strukturene skapt etter den kalde krigens slutt ikke nødvendigvis klarer å skape sammenheng og forståelse for dagens sikkerhetsutfordringer, fordi strukturene er preget av en tankegang om separate «eksterne» og «interne» utfordringer (Löjdquist, 2019).

Sverige var det første nordiske landet til å introdusere en modell for psykologisk forsvarsplanlegging etter andre verdenskrig – også før etableringen av totalforsvarsmodellen. Dette omfatter mottiltak mot desinformasjon, som Sverige i likhet med Finland, har i kjernen av i sitt totalforsvarskonsept. I tillegg kommer militært forsvar, økonomisk forsvar og sivilt forsvar. Statsminister Stefan Löfven annonserte på Folk og Forsvars sikkerhetskonferanse i 2018 at det skulle bli etablert en offentlig etat for å arbeide med koordinering av aktiviteter forbundet med psykologisk forsvar (Wigell *et al.*, 2021). Myndigheten för psykologiskt försvar ble deretter opprettet i 2022. Av andre tiltak har også offisielle svenske medier samlet seg om et initiativ for å adressere falske nyheter, noe som har resultert i nettsiden Faktiskt.se (Wigell et al., 2021).

I oktober 2022 besluttet Sveriges nye regjering å flytte ansvaret for samfunnssikkerhet fra Justisdepartementet til Forsvarsdepartementet. Regjeringen besluttet også å opprette et nasjonalt sikkerhetsråd. Hensikten med endringen er ifølge statsminister Kristersson å bygge motstandskraft mot hybride trusler og øke cybersikkerheten etter en tid hvor den sivile siden av totalforsvaret har vært forsømt (Kristersson, 2022).

5.3 Estland

Estland baserer seg, som Finland, på et «*Comprehensive Security Concept».* Etter uavhengigheten fra Sovjetunionen i 1991, ble Nato-medlemskap ansett som den viktigste sikkerhetsstrategien for Estland. Samtidig førte svensk og finsk innflytelse på forsvarsplanlegging til at territorial- og totalforsvarskonseptet fant veien inn i det estiske forsvaret. Det ble fastslått at forsvaret måtte utvikles på en slik måte at militæret kunne støtte sivile myndigheter i tilfeller av tekniske ulykker, naturkatastrofer, epidemier og andre katastrofer (Maskaliunate, 2020; Veebel & Ploom, 2018). På mange måter fulgte den estiske forsvarsorganiseringen de finske løsningene, blant annet ved at en beholdt verneplikten, oppmuntret til frivillig deltakelse og introduserte forsvarskurs for å styrke det sivil-militære samarbeidet (Maskaliunate, 2020; Szymański, 2020). I de estiske forsvarsstrategiene fra 2011 og 2017 ble det konstatert at nasjonalt forsvar ikke lenger kan begrenses til å gjelde militært forsvar alene, og at militære krefter må kombineres med ikke-militære kapabiliteter for å motvirke hybride trusler i krig og fredstid (Forsvarsdepartementet (Estland), 2011; Veebel & Ploom, 2018).

Siden 2017 har Estland operert med et «*Comprehensive National Defence Concept»*, som kombinerer militære kapabiliteter med aktiviteter og ressurser fra offentlig og privat sektor, i tillegg til sivilsamfunnet (Regjeringen (Estland), 2017). Det estiske forsvarskonseptet bygger hovedideen på en integrert tilnærming, hvor koordinering og interaksjon mellom ulike departementer og organisasjoner prioriteres med et mål om å generere en samlet respons under en potensiell krise (Veebel & Ploom, 2018). Estland baserer med andre ord forsvars- og sikkerhetspolitikken på en helhetlig samfunnstilnærming (Forsvarsdepartementet (Estland), u.å.; Regjeringen (Estland), 2017; Veebel & Ploom, 2018).

I dagens sikkerhetskonsept fremheves det at truslene er blitt mer komplekse eller sammensatte, og kildene mer varierte. Asymmetriske trusler som ikke følger landegrenser, og der kilden er vanskelig å spore, har dukket opp, og disse truslenes innvirkning på sikkerheten kan sammenlignes med tradisjonelle sikkerhetstrusler. Det blir i økende grad tydelig at sikkerhet påvirkes av økonomisk ustabilitet, utvikling i det digitale rom, teknologiske trusler, radikalisering og terrorisme, organisert kriminalitet og korrupsjon, migrasjonsstrømmer, i tillegg til en variasjon av andre kriser (Regjeringen (Estland), 2017, s. 5). I de nasjonale forsvarsdokumentene nevnes hybride trusler kun i forordet til forsvarsstrategien fra 2011 (Brânda & Saulic, 2020), men defineres ikke.

Cyberangrep og bronsesoldatkrisen (2007)

I 2007 ble det bestemt at det sovjetiske krigsminnesmerket, Bronsesoldaten, skulle flyttes fra Tallin til en militær kirkegård. Avgjørelsen førte til sammenstøt mellom russiske og estiske nasjonalister. I de påfølgende dagene opplevde Estland økonomisk og diplomatisk press fra Russland, heriblant krav om at den estiske regjeringen måtte trekke seg, blokade og angrep på den estiske ambassaden i Moskva, samt en aggressiv mediedekning. På sosiale medier, i forum og på mediekanalers hjemmesider florerte manipulerte bilder av en oppkuttet bronsestatue. Samtidig ble Estland utsatt for en rekke cyberangrep der estiske mediehus, banker, og statlige institusjoner særlig ble rammet (Juurvee & Arold, 2021; Juurvee & Mattiisen, 2020). Angrepet anses gjerne som det første cyberangrepet utført av et land mot et annet (Juurvee & Mattiisen, 2020). Angrepet belyste i tillegg utfordringene med å identifisere en proporsjonal respons på et angrep i det digitale rom. Nato har erkjent utfordringer med å definere *hva* som utgjør terskelen for respons, og *hvordan* en skal reagere. Dette fører til tydelige forskjeller i fortolkning. Estiske beslutningstakere anså angrepet som en åpenbar hjemmel for Natos artikkel fem, mens Nato var av en annen oppfatning (Kristiansen & Hoem, 2019, s. 258).

Trusler og utfordringer beskrives årlig i rapporter fra *Estonian Internal security Service* og *Estonian Foreign Intelligence Service (*EFIS) (Szymański, 2020). EFIS ligger under forsvarsdepartementet, og samler, analyserer og rapporterer informasjon om Estlands eksterne sikkerhetstrusler (Forsvarsdepartementet (Estland), 2021). Informasjonen som samles av EFIS har en betydelig innflytelse på utforming av sikkerhetspolitikken, og er en viktig del av det nasjonale forsvaret (Estonian Foreign Intelligence Service, u.å.). Samtidig sørger *Estonian Internal Security Service,* som ligger under innenriksdepartementet, for å identifisere, overvåke, påvirke og hindre etterretningsvirksomhet og spionasje i Estland (Kaitsepolitseiamet, u.å.). I trusselvurderingene rettes oppmerksomheten især mot russiske trusler i form av propaganda mot den russiske minoriteten i Estland, desinformasjon, angrep i det digitale rom, økt russisk militært nærvær i Østersjøen og aggresjon i Ukraina. I trusselvurderingen fra 2022 anses en militær offensiv mot Estland og de baltiske statene som lite sannsynlig, men ulike typer av hybride kriser som sannsynlig (Estonian Foregin Intelligence Service, 2022; Szymański, 2020).

I langtidsplanen for det estiske forsvaret 2013–2022, deles planen for første gang opp i en militær del og en ikke-militær del (*National defence development plan* og *Non-military parts of the national defence development plan*). Dette innebærer at de følgende områdene anses som sentrale for nasjonalt forsvar og skal videreutvikles sammen med det militære aspektet: (1) sivil støtte til militæret, (2) internasjonal aktivitet, (3) intern sikkerhet, (4) kritiske samfunnsfunksjoner og (5) psykologisk forsvar. Av tiltak fremmes oppsett av et mobiliseringsinformasjonssystem, kontraktinngåelse med private aktører vedrørende varer til beredskapslager, regelmessige øvelser med sivile resurser, økt kapasitet til politi, grensevakt og redningstjeneste. Elektroniske kapabiliteter og kontrollsystem skal videreutvikles, kommunikasjonssystem og den medisinske beredskapen skal styrkes, kurs i psykologisk forsvar og myndighetenes evne til å identifisere fiendtlig propaganda skal videreutvikles, og beredskap forbedres i kriser med større kommunikasjonsbehov (Regjeringen (Estland), u.å.).

Forsvarsdepartementet er ansvarlig for utviklingen av militært forsvar og for sivil støtte til forsvaret. Utenriksdepartementet er ansvarlig for internasjonale aktiviteter, innenriksdepartementet er ansvarlig for intern sikkerhet, herunder kontinuerlig opprettholdelse av stat og samfunn, og regjeringskontoret er ansvarlig for strategisk kommunikasjon og psykologisk forsvar (Veebel & Ploom, 2018). Den nasjonale sikkerhets- og forsvarskoordinasjonsenheten rådfører statsministeren i nasjonale sikkerhetsspørsmål, organiserer sakene til regjeringens sikkerhetskomité, og koordinerer nasjonal sikkerhet og forsvarsledelse (Regjeringen (Estland), 2020). Enheten har utover dette ansvar for å koordinere de estiske sikkerhets- og etterretningsbyråene, forsvarsplanleggingen samt å sikre regjeringens situasjonsforståelse (Szymański, 2020). Til tross for at koordinering mellom ulike departementer og organisasjoner skal prioriteres, viser en studie fra *Estonian National Defence College* at integrering og koordinering er mer synlig på departementsnivå og i den politiske ledelsen enn på «spesialist»-nivå. Her oppstår derfor en *siloeffekt* ettersom deling av krisescenarioer, kritisk respons og kombinering av ressurser ikke praktiseres daglig (Veebel & Ploom, 2018).

I sikkerhetskonseptet fra 2017 blir *motstandsdyktighet* (*kerkus* på estisk) for første gang presentert, og mange av målene i konseptet er rettet mot å oppnå et motstandsdyktig samfunn. Motstandsdyktighet defineres som samfunnets evne til rask gjenopprettelse etter krise (Szymański, 2020). Dette oppnås gjennom en kombinasjon av troverdig beskyttelse av sivile, innbyggernes psykologiske styrke, og trygge sosiale og fysiske omgivelser (Regjeringen (Estland), 2017). I 2018 godkjente regjeringen et sivilt beskyttelseskonsept som tydeliggjør at hele samfunnet må bidra i krise og krig. Her anbefales alle husstander å ha sitt eget beredskapslager slik at de klarer seg selv i minst én uke. Av tiltak fremmes undervisning i kriseberedskap for elever i grunnskolen, distribusjon av informasjon om kriseberedskap og om oppførsel under kriser, en nasjonal kriselinje samt psykososial støtte til innbyggerne i etterkant av en krise. I tillegg skal folkets evne til beredskap testes jevnlig i undersøkelser (Regjeringen (Estland), 2018).

Psykologisk forsvar er en viktig faktor for å oppnå motstandsdyktighet i samfunnet, og oppnås ved å informere og øke bevisstheten i samfunnet vedrørende informasjonsrelaterte aktiviteter som kan skade den rettsstatlige ordenen og samfunnets verdier (Regjeringen (Estland), 2017).

Estland har satt i gang en rekke tiltak for å beskytte staten og samfunnet mot påvirkningsoperasjoner, heriblant å forbedre sitt strategiske kommunikasjonssystem. Flere statlige og frivillige organisasjoner jobber aktivt med å forbedre motstandsdyktighet mot russisk desinformasjon og falske nyheter. Myndighetene og ulike grupper observerer innhold i media, på tv og generell trafikk på internett, med et mål om å fange opp trender. Resultatene publiseres regelmessig for å øke folkets situasjonsbevissthet. I tillegg er det opprettet en statlig russisk tv kanal, ETV+, rettet mot den russiske diasporaen i Estland som et alternativ til de russiske tv-kanalene som opererer i landet. Det strategiske kommunikasjonssystemet fungerer ikke optimalt, og det har oppstått problemer med overregulering, langsomme beslutningsprosesser og dobbeltarbeid (Veebel *et al.*, 2022).

Estland anses som et velutviklet digitalt samfunn og har i løpet av de siste tiårene utviklet cybersikkerhet til å bli et sentralt kompetanseområde. Estland huser Natos *Cooperative Cyber Defence Center of Excellence* og produserer den internasjonalt anerkjente *Tallin manual*, som presenterer retningslinjer og juridiske rammeverk for cybersikkerhet (Chana, 2021). Den estiske cybersikkerheten baserer seg på et nært og tillitsfullt samarbeid mellom offentlig og privat sektor, der også involveringen av frivillige og sivilsamfunnet spiller en viktig rolle (Regjeringen (Estland), 2017). Ett av tiltakene har vært en opprettelse av en frivillig *Cyber Defence League* som består av ledende IT-eksperter som har oppdrag i å beskytte Estlands *high-tech way of life* – noe som innebærer å beskytte informasjonsinfrastruktur og støtte nasjonalt forsvar (Kaitseliit, 2022). Estland organiserer cybersikkerhet enhetlig, og bruker de samme strukturelle løsningene både i fred og krig (Regjeringen (Estland), 2017).

e-Estonia

I 1993 ble prosjektet e-Estonia lansert med et mål om å skape en digital statlig infrastruktur. I dag er prosjektet ansett som et globalt eksempel på hvordan en planlegger, utvikler og operasjonaliserer en digital transformasjon i samfunnet. Samtidig har Estland høstet kritikk for hvordan prosjektet er innrettet. Prosjektet krever en type medvirkning fra innbyggerne som mange mener bygger på ettergivenhet. I tillegg argumenterer noen for at programmet, som er obligatorisk, er invaderende og overdrevet retningsgivende (Chana, 2021).

5.4 Storbritannia

Storbritannia har blitt kritisert for å være utydelig i begrepsbruken når det kommer til sammensatt virkemiddelbruk. Både gråsoneaktiviteter, hybridkrig og hybride trusler har blitt brukt om hverandre uten tydeliggjøring av hva forskjellen mellom begrepene innebærer (Janičatová & Mlejnková, 2021; Rauta & Monaghan, 2021). Til tross for den uklare begrepsbruken er det tydelig at Storbritannia ser på at utfordringsbildet er preget av svakere skillelinjer mellom krig og fred, i tillegg til at teknologi bidrar til nye sårbarheter blant annet på internett. Det ble i Storbritannias integrerte gjennomgang av sikkerhets-, forsvars-, utviklings- og utenrikspolitikk uttrykt

behov for å tenke mer helhetlig rundt problemstillingene, ettersom det er vanskelig å møte disse utfordringene gjennom en «nasjonal sikkerhet» og en «forsvarsagenda» alene (Statsministerens kontor (Storbritannia), 2021, s. 70).

I tillegg til utydelig begrepsbruk har Storbritannia blitt kritisert for et stort gap mellom skarp ordbruk og påfølgende håndtering i form av tiltak og politikkutforming. Også sammenlignet med andre land i Norden, Baltikum, USA og Australia har Storbritannia ligget bak når det gjelder mottiltak og fleksible samarbeidsordninger (Rauta & Monaghan, 2021). Den integrerte gjennomgangen av sikkerhets-, forsvars-, utviklings- og utenrikspolitikk har bidratt til å øke tverrsektorielt samarbeid og forståelse (Rauta & Monaghan, 2021; Statsministerens kontor (Storbritannia), 2021).

Forskning viser at forsvarsdebatten om Russland i Storbritannia i perioden 2014–2019 var preget av ikke-militære trusler og undergravende aktiviteter. Informasjons- og cyberkrig ble ofte fremhevet som utfordringer i forbindelse med sammensatte trusler. Britiske folkevalgte har i stor grad fremhevet konvensjonelle styrker som svar på disse utfordringene (Janičatová & Mlejnková, 2021). Statlige forsvarsaktiviteter (60 tiltak), cyberkrig (49 tiltak) og modernisering/investering (39 tiltak) var forsvarstiltakene som oftest ble nevnt. Økonomiske (82) tiltak var den kategorien mottiltak som ble nevnt flest ganger blant ikke-forsvarsrelaterte tiltak. I forbindelse med internasjonalt samarbeid ble Nato ble nevnt 115 ganger i kontrast med FN, som bare ble nevnt 7 ganger (Janičatová & Mlejnková, 2021, s. 330).

Statsministerens kontor erkjenner at en ikke har anledning til å besvare hver eneste trussel. Det foreligger derfor en intensjon om å gjøre det vanskeligere og dyrt for fremmede aktører å ramme Storbritannia. Dette skal gjøres gjennom å redusere sårbarheter og øke motstandsdyktighet (Statsministerens kontor (Storbritannia), 2021).

Rauta og Monaghan (2021) skriver at blant tiltakene mot sammensatt virkemiddelbruk er det i stor grad militærmakt og cybersikkerhet som er fremhevet. Investeringer i de tre forsvarsgrenene har hatt som hensikt å bidra til avskrekking. Disse tiltakene fremstår som frakoblet fra forsvarsdebattene i 2014–2019 som i hovedsak fremhevet de ikke-militære utfordringene (Janičatová & Mlejnková, 2021).

Ved sammensatt virkemiddelbruk, eller såkalt gråsoneproblematikk, blir forgiftningen i Salisbury trukket frem som et eksempel på en aktivitet som kan inngå i konseptet «sammensatte trusler». Storbritannias håndtering av denne hendelsen har blitt fremhevet som en suksess, blant annet fordi britiske myndigheter raskt kunne tilskrive handlingen til Russland og dermed motvirke en desinformasjonskampanje i forbindelse med hendelsen. Det har blitt understreket at håndteringen av hendelsen også var en suksess fordi håndteringen baserte seg på informasjon og ikke gjengjeldelse. Stewart hevder at en har med andre ord ikke ofret egen moral eller egne prinsipper i håndteringen (Stuart, 2022).

Forgiftningen av Sergei Skripal i Salisbury (2018)

Søndag 4. mars 2018 ble Sergei Skripal (66) og hans datter Yulia (33) funnet bevisstløse på en parkbenk i den britiske byen Salisbury. De hadde blitt forgiftet med nervegift og havnet i koma etter hendelsen, men overlevde angrepet. Tilfeldige personer kom over beholderen i ettertid av hendelsen og én av disse døde. For å skape forvirring rundt hendelsen publiserte de russiske mediene Russia Today (RT) og Sputnik over 735 artikler om temaet og lanserte totalt 138 separate teorier om det som hadde skjedd (Ramsay & Robertshaw, 2019, s. 22). Sergei Skripal hadde tidligere vært russisk etterretningsoffiser, men har i Russland blitt dømt for å ha spionert på vegne av Storbritannia. Allerede 12. mars sa daværende statsminister Theresa May at Russland med stor sannsynlighet lå bak angrepet. Kort tid etter ble 23 russiske diplomater utvist fra Storbritannia, hvorpå Russland utviste 23 britiske diplomater fra Russland. De to russiske agentene fra den militære etterretningstjenesten GRU, som gikk under aliasene Alexander Petrov og Ruslan Boshirov, ble siktet for angrepet. Russland har avvist anklagene om at de var involvert (Ramsay & Robertshaw, 2019; Roth, 2018; Stewart, 2022).

Det bør fremheves at Storbritannia har foreslått en rekke andre tiltak for å møte dagens utfordringer. Ikke alle disse tiltakene blir forslått spesifikt for å bekjempe sammensatte trusler, men kan likevel forstås som tiltak som bidrar til å motvirke sammensatt virkemiddelbruk. Dette innebærer, men er ikke begrenset til å: øke tverrsektorielt samarbeid, juridisk reform for etterretnings- og sikkerhetstjenester, øke bidrag til å bekjempe desinformasjon både ute og hjemme, sette diplomati i sentrum, bygge internasjonale koalisjoner for å kunne attribuere trusler og styrke cybersikkerhet (Statsministerens kontor (Storbritannia), 2021).

Storbritannias etterretningsvirksomhet er delt inn i utenlandsk (MI6) og innenlandsk (MI5) etterretning (SIS, u.å.). I tillegg er Storbritannia en del av en etterretningsallianse med USA, Canada, Australia og New Zealand som heter *Fives Eyes*. Denne alliansen muliggjør utveksling av informasjon på tvers av grensene (NCSC, u.å.). I 2021 ble Storbritannia dømt i EMD i Strasbourg for brudd på retten til ytringsfrihet, privatliv og familieliv i *Big Brother Watch v. Storbritannia*. Saken omhandlet digital nettovervåking og bulkinnsamling av grenseoverskridende informasjon, hvor det blant annet ble påpekt mangler vedrørende uavhengig kontroll. Dette illustrerer noen av utfordringene knyttet til etterretning i dagens digitaliserte samfunn (Grand Chamber ECtHR, 2021a; NIM, 2021; Zalnieriute, 2022).

Ett av tiltakene Storbritannia har gjort er utviklingen av et verktøysett for å motvirke desinformasjon, kalt RESIST 2 (*Recognise, Early Warning, Situational Insight, Impact Analysis, Strategic Communications, Tracking Effectiveness*). Verktøysettet er laget av den britiske regjeringen og er ment for organisasjoner og aktører som ønsker å beskytte publikummet sitt og organisasjonen sin mot mis- og desinformasjon. Hensikten med dette verktøysettet er å bidra til forståelse for hvordan mis- og desinformasjon kan identifiseres, takles, besvares og motvirkes, slik at effekten av uønsket informasjonspåvirkning på befolkningen reduseres (Pamment, 2021).

5.5 Nederland

Til tross for forskjeller i sikkerhetsorganisasjonen har Nederland og Finland relativt lik tilnærming til sammensatte trusler. I Nederland har regjeringen ansvar for å motvirke sammensatte trusler, men jobber i økende grad sammen med andre samfunnsaktører. Koordineringen skjer gjennom en nasjonal koordinator (National Coordinator for Counterterrorism and Security (NCTV)) sammen med Forsvarsdepartementet, Utenriksdepartementet og Justis- og sikkerhetsdepartementet. Regjeringen samarbeider også med private aktører, sivilsamfunnet, samt teknologiske og akademiske miljøer for cybersikkerhet og kritisk infrastruktur. Problemstillinger tilknyttet blant annet sammensatte trusler diskuteres i tverrsektorielle strukturer hvor alle departementene deltar. Andre relevante aktører blir invitert inn ved behov. NCTV har etablert flere programmer, hvor hybridkrig inngår som et av disse. I tillegg er det etablert programmer på utenlandsk innblanding, desinformasjon, økonomisk sikkerhet og kritisk infrastruktur i NCTV (Wijnja, 2022).

Nederland har, i likhet med Storbritannia, brukt forskjellig terminologi for å beskrive sammensatte trusler. Dette inkluderer blant annet hybridkonflikt, hybrid maktkamp, hybride trusler og operasjoner i en hybrid kontekst. Nederland har også erkjent at sammensatte trusler er et økende problem, samt at en ikke lenger kan begrense fokus til kun én type trussel eller operasjon. I den forbindelse blir befolkningen fremhevet som en viktig ressurs (Forsvarsdepartementet (Nederland), 2022).

I 2018 ga det nederlandske utenriksdepartementet ut en sikkerhetsstrategi for perioden 2018–2022.[14] I denne strategien fremheves det blant annet at sammensatte virkemidler, cyberangrep og påvirkningsoperasjoner er et problem – spesielt i lys av rask teknologisk utvikling. Nederlands strategi omfatter tre steg: å forebygge, forsvare og styrke. Strategien fremhever blant annet forskning som viser at 1 euro investert i sikkerhetsforebygging kan spare 16 euro i kostnaden av å reparere. Sterk etterretnings- og informasjonskapabilitet er derfor viktig (Utenriksdepartementet (Nederland), 2018, s. 25).

De uttalte største truslene for Nederland er cyberangrep, uønsket utenlandsk innblanding og undergravingsaktiviteter, militære trusler, angrep på kritiske beslutningsprosesser og CBRN[15] (Wijnja, 2022). Et eksempel på slik uønsket utenlandsk aktivitet var da fire russiske GRU-spioner i 2018 ble avslørt i forbindelse med en cyberoperasjon på Organisasjonen for forbud mot kjemiske våpen (OPCW) (BBC News, 2018). I tillegg kommer den mer særegne trusselen for Nederlands fysiske sikkerhet, nemlig problemstillinger knyttet til vann. Dette innebærer cybersikkerhet i forbindelse med tunneler, broer, dammer og sluser (Wijnja, 2022).

[14] I juli 2022 etterlyste den nederlandske utenriksministeren og forsvarsministeren etterlyste mer informasjon og råd for å motvirke sammensatt virkemiddelbruk, innenfor rammene av demokrati og rettsstatsprinsipper. Frist for å svare på denne utlysningen er utgangen av 2022. (Forsvarsdepartementet (Nederland) og Utenriksdepartementet (Nederland), 2022).

[15] CBRN er en fellesbetegnelse på hendelser som omfatter kjemiske stoffer (C), biologiske agens (B), radioaktive stoffer (R) og nukleært materiale (N) med høyt farepotensiale (Justis- og beredskapsdepartementet *et al.*, 2016, s. 3).

Et avslørt cyberangrep på OPCW (2018)

Den 10. april 2018 reiste fire russiske personer på diplomatiske pass fra Moskva til Amsterdam. Tre dager senere blir de fire mennene arrestert utenfor OPCWs hovedkvarter i Haag og utvist samme dag. Bilen de ble arrestert i var utstyrt med datamaksiner, WiFi-paneler og antenner direkte rettet mot OPCW. I tillegg hadde de fire mennene en stor sum kontanter (20.000 euro) og en rekke forskjellige type telefoner med seg, som én av mennene forsøkte å ødelegge da de ble arrestert. En av datamaskinene inneholdt spor etter forsøk på å påvirke etterforskningen av nedskytningen av det malaysiske passasjerflyet MH17 over Øst-Ukraina i 2014. OPCW undersøkte på tidspunktet nervegiften som ble benyttet til å forgifte Sergei Skripal i Salisbury, Storbritannia, samt anklagene om kjemiske angrep i Douma, Syria. Russland har avvist spion- og cyberangrepsanklagene (BBC News, 2018; Smith-Spark & Polglase, 2018).

Nederland har i nyere tid investert mer i sine etterretningstjenester og endret strukturen (Friis & Hansen, 2020). I tillegg har juridiske endringer blitt gjennomført slik at tjenestene kan avdekke cyberangrep tidligere. Den endrede loven gjør at tjenestene blant annet kan innhente data fra datakabler (Rijksoverheid 2020 i Wijnja, 2022). Nederlands etterretningsenhet AIVD (*General Intelligence and Security Service*) innhenter informasjon både innenlands og utenlands om spørsmål rundt blant annet terrorisme, ekstremisme, fordekte innblandingsaktiviteter og fremheving av nasjonal sikkerhet (AIVD, 2018, u.å.-a, u.å.-b). I tillegg har Nederland en forsvarsetterretning og sikkerhetsenhet, DISS (Defence Intelligence and Security Service), som bistår det nederlandske forsvaret (Forsvarsdepartementet (Nederland), 2019).

Regjeringen har gjennomført tiltak for å begrense effektene av desinformasjon, fremfor å aktivt motsi eksisterende falske nyheter. I 2019 hadde regjeringen blant annet en kampanje for å øke forståelsen blant befolkningen for desinformasjon, samt skape forståelse for hvordan man skal kunne gjenkjenne falske nyheter. Det kan likevel potensielt være vanskeligere å øke motstandsdyktigheten i befolkingen i Nederland sammenlignet med Finland ettersom trusselen ikke er tydelig og synlig (Wijnja, 2022).

Nederland har i tillegg gjennomført tiltak for å øke samarbeid nasjonalt og internasjonalt med likesinnede som et ledd i å øke felles situasjonsforståelse. Det fremheves spesielt muligheter for samarbeid med EU og Storbritannia (Wijnja, 2022). I tillegg til disse tiltakene har Nederland økt investeringen i Forsvarsdepartementet for å styrke sine defensive kapabiliteter. Alliansepolitikken gjennom både Nato og EU står fortsatt sterkt (Wijnja, 2022).

Når det kommer til å besvare sammensatte trusler har Nederland i likhet med Finland uttalt at responsen avhenger av konteksten for hybride angrepet. Det har blitt vektlagt å vurdere alle dynamikker og konsekvenser av eventuelle besvarelser eller motangrep. Nederlenderne har likevel uttalt at det er mulig, hvis nødvendig, å besvare sammensatte trusler med et bredt spekter av tilgjengelige virkemidler (Utenriksdepartementet (Nederland), 2018; Wijnja, 2022).

I 2022 fremhevet det nederlandske forsvarsdepartementet seks tiltak som vil være viktig for det nederlandske forsvaret i tiden fremover. Dette innebar sterk (økonomisk) støtte, å være en god arbeidsgiver som en del av samfunnet, styrket spesialisering, mer europeisk samarbeid, nye domener og muligheter til innovasjon, og informasjonsdrevet organisasjon og operasjon (Forsvarsdepartementet (Nederland), 2022).

5.6 Australia

Australia skiller seg fra de andre landene i denne studien ved at Kina har en mer fremtredende rolle i utfordringsbildet. Kina har blant annet brukt kombinasjoner av virkemidler innenfor økonomi, cyber, informasjon og politikk for eksempelvis å skape splid mellom Australia og deres allierte, og for å øke støtten til Beijing blant den kinesiske diasporaen i Australia (Barber, 2017; Forsvarsdepartementet (Australia), 2020; Wigell *et al.*, 2021). I motsetning til det en refererte til som «små grønne menn» på Krim, har en i Australia heller erfaring med såkalte «små blå menn» som blir brukt for å kontrollere Sør-Kina-havet (Seebeck *et al.*, 2022). Likevel har en mer tradisjonell form for sikkerhet stått sentralt i Australias sikkerhetspolitikk inntil nylig (Buchanan, 2019).

I 2017 hevdet kaptein og etterretningsoffiser Nicholas Barber at lite hadde blitt gjort i Australia for å motvirke sammensatte trusler, men siden da har flere tiltak blitt innført. Australia har blant annet innført en rekke nye lover og byråkratiske strukturer for å hindre utenlandsk innblanding – spesielt fra kinesiske aktører (Barber, 2017; Wigell *et al.*, 2021). Australia har også tatt grep for å begrense desinformasjon gjennom flere juridiske endringer (blant annet gjennom '*Code of Practice on Disinformation and Misinformation'*, '*the Foreign Influence Transparency Scheme Bill'* (FITS) og '*the Espionage and Foreign Interference Bill'*) (Wigell *et al.*, 2021). Fokuset har vært å kriminalisere, forstyrre og avskrekke den mest skadelige formen for påvirkning og innblanding (Mansted, 2021). Et grep som har blitt gjort for å kunne skille mellom legitimt offentlig diplomati og illegitim desinformasjon, er etableringen av et register. Alle aktører, individer som enheter, som uttaler seg på vegne av utenlandske aktører må registrere seg i et offentlig register. Dette kan for eksempel være parlamentarisk lobbyisme og kommunikasjonsaktiviteter. Tidligere statsråder omfattes også av et slikt register, samt ytterligere regler for åpenhet. Dette skal bidra til å belyse hvem som står bak opplysninger som blir gitt, samt utvider mulighetene for å etterforske de aktørene som ikke registrerer seg (Hutchens, 2018).

Mansted (2021) fremhever at fordelen med denne forholdsvis smale formen for mottiltak mot sammensatte trusler er for å ikke gå for langt i sikkerhetstenkningen og dermed risikere å overmilitarisere samfunnet, i beskyttelsen mot utenlandsk påvirkning samt beskytte politisk ytringsfrihet. En vil dermed bidra til beskyttelse mot sammensatte virkemidler, uten at det går på bekostning av demokratiske verdier som åpenhet og ytringsfrihet. Videre anbefaler Mansted (2021, s. 1–2) blant annet at Australia bør vektlegge åpenhet, prioritere demokratiske politiske og sosiale rettigheter, støtte et robust og uavhengig media og utvide rapporteringsforpliktelser av utenlandske aktører.

Australia har satt i gang vurdering av sårbarheter i kritiske infrastrukturer, inkludert cybersystemer, for å motvirke sammensatt virkemiddelbruk og øke motstandsdyktighet (Buchanan, 2019). En helhetlig samfunnstilnærming har blitt sett på som nødvendig ved vurdering av kritiske samfunnsfunksjoner, fordi de i økende grad eies av private aktører. Å skape situasjonsforståelse gjennom informasjonsflyt har blitt adressert gjennom *Trusted Information Sharing Network* (TISN), som ligger under innenriksdepartementets *Critical Infrastructure Centre* (CIC) (Wigell *et al.*, 2021). Andre tiltak inkluderer etableringen av *Foreign Interference Threat Assessment Centre* i Australias sikkerhets- og etterretningsorganisasjon (ASIO) og utvikling av et rammeverk for å motvirke utenlandsk innblanding i universitetssektoren. I tillegg har det blitt igangsatt tiltak for å øke kunnskapen blant unge om medievitenskapen (Wigell *et al.*, 2021). Det har også blitt fremmet forslag om å sette opp et indopasifisk hybrid trussel-senter bygget på samme struktur som Hybrid CoE-senteret i Helsingfors (Seebeck *et al.*, 2022).

«Små blå menn» i Sør-Kina-havet

I Sør-Kina-havet har Kina bygget 28 kunstige øyer som har blitt militarisert, til tross for at Bejing har gitt et løfte om at de omstridte øyene ikke skulle bli militarisert (Page et al., 2015; Seebeck et al., 2022). Den amerikanske tankesmien Center for Strategic and International Studies (CSIS) har laget en oversikt over øyene som viser utviklingen over tid (CSIS, n.d.). I tillegg har Kina benyttet både kystvakt og fiskebåter, med støtte fra militære styrker, for å forstyrre andre staters tilstedeværelse i området (Guilfoyle & Chan, 2022; Seebeck et al., 2022). Den Australske tankesmien Australian Strategic Policy Institute (ASPI) har beskrevet denne aktiviteten som beslektet med «små grønne menn» slik en så under annekteringen av Krimhalvøya, men at det i Sør-Kina-havet blir beskrevet som «små blå menn». I kombinasjon med økonomisk tvang og cyberangrep har Kina oppnådd kontroll over 12,92 km^2 nytt land i regionen, samtidig som militær konfrontasjon har blitt unngått (Seebeck et al., 2022, s. 16). Det australske forsvarsdepartementet (2020) har uttalt at de registrerer Kinas økende jakt på makt og innflytelse i regionen og er bekymret for at det skal undergrave stabiliteten.

For å forbedre den helhetlige tilnærmingen på regjeringsnivå etablerte Australia *National Counter Foreign Interference Coordinator* (NCFIC) i innenriksdepartementet i 2018. NCFICs ansvar er å samarbeide med etterretningstjenesten for å få situasjons- og konsekvensforståelse, koordinere tiltak nasjonalt og internasjonalt, koordinere rådgivning til sektorer og systemer som har risiko for utenlandsk innblanding og øke engasjement i kulturelt og språklig forskjellige miljøer for å styrke evnen til å identifisere manipulasjon fra fremmede aktører (Wigell *et al.*, 2021). Spesielt Australias nordlige områder påpekes som sårbare for utenlandsk innblanding, fordi en i likhet med Krimhalvøya har sett historisk vold mot urbefolkningen som kan bli benyttet til å skape splid i samfunnet (Barber, 2017; Wigell *et al.*, 2021). Til tross for at Australia er tydelig på at militærmakt skal brukes ved nødvendighet, har Australias forsvarsdepartement påpekt at å identifisere tydelige terskler for militær respons innen spesielt innen det digitale rom og romdomenet er vanskelig fordi de mangler tydelige grenseoverganger (Forsvarsdepartementet (Australia), 2020).

Etterretningsarbeidet i Australia har en egen enhet som jobber med hemmelig etterretningsinnhenting i utlandet, *Australian Secret Intelligence Service* (ASIS), men Australia har også en enhet som jobber med innhenting og vurdering av etterretning i både inn- og utland, *Australian Security Intelligence Organisation* (ASIO) (ASIS, u.å.). Australia er, i likhet med Storbritannia, også medlem av etterretningsalliansen *Five Eyes.* Dette er en etterretningsallianse mellom Storbritannia, USA, Canada, Australia, og New Zealand som muliggjør utveksling av informasjon på tvers av grensene (NCSC, u.å.).

EU ønsker å lære fra Australia

En delegasjon fra EU-parlamentet var i september 2022 på besøk i Australia for å lære om hvordan de håndterer fremmedstatlig innblanding. Delegasjonen var mest interessert i å lære mer om hvordan Australia gjennomgår utenlandske investeringer i kritisk infrastruktur, håndtering av desinformasjon og undersøkelser om hvordan universiteter kan være mål (Nicholson, 2022).

6 Hva kan Norge lære av andre land?

Dette kapittelet knytter sammen foreslått mønsterpraksis for Nato og EU og de enkelte landenes forskjellige fremgangsmåter for å avskrekke, avdekke og håndtere sammensatte trusler. Sammenstillingen av funnene, illustrert i en oversikt i tabell 6.1, gir eksempler på tiltak som er innført i Finland, Sverige, Estland, Storbritannia, Nederland og Australia. Dette kapittelet gir ingen utfyllende liste over tiltak, men bidrar til å belyse de forskjellige tilnærmingene og hvordan de kan være relevante for Norge.[16]

Tiltakene er organisert i kategoriene avskrekking, avdekking og håndtering. Vi baserer oss på MCDC-arbeidet ved begrepsbruken av avskrekking, avdekking og håndtering (respons), fordi denne gruppen har utviklet et helhetlig rammeverk for å motvirke sammensatte trusler. Med «avskrekke» mener vi tiltak som blir igangsatt for å gjøre stater og befolkningen mindre sårbare for angrep – med andre ord forebygging. Forebyggende tiltak vil dermed også være tiltak som omfatter økt motstandsdyktighet og avskrekkingsstrategier i form av nektelse og trusler om mulig straff. Å «avdekke» refererer til tiltak som øker situasjonsforståelsen av hva som har skjedd og bidrar til en evne til å tilskrive handlinger til aktører. Dette omfatter i stor grad etterretningsvirksomhet, men også andre type tiltak som bidrar til å identifisere aktørene som står bak handlinger (Monaghan *et al*., 2019, s. 3). Med «håndtering» refererer vi til tiltak som bidrar til besvare handlinger, det vil si respons på hendelser som har skjedd. Dette kan for eksempel være krisehåndteringstiltak, men også tiltak som blir igangsatt på et lavere nivå i krisespekteret (Monaghan *et al*., 2019, s. 4). I MCDC-arbeidet inkluderes også tiltak for å identifisere sårbarheter i den sistnevnte kategorien, men i denne rapporten begrenser vi forståelsen av «håndtering» til hendelseshåndtering. Identifisering og lukking av sårbarheter er omfattet av kategorien «avskrekke».

[16] For informasjon om Norges tilnærming til sammensatte trusler viser vi til Meld. St. 5 (2020–2021, s. 93) og Meld. St. 10 (2021–2022).

Tabell 6.1 Eksempler på tiltak mot sammensatte trusler i utvalgte land. Tabellen er ment som et overblikk og er ikke en uttømmende eller gjensidig utelukkende liste over eksempler.

	Finland	**Sverige**	**Estland**	**Storbritannia**	**Nederland**	**Australia**
Organisering	'Comprehensive Security Concept'	Totalforsvar	'Comprehensive Security Concept'	'Integrated Approach'	'Integrated International Security Strategy'	Forsvarsstrategi basert på *shape*, *deter*, *respond*
Avskrekke	Sikre fritt, mangfoldig og ansvarlig media	Psykologisk forsvar	Psykologisk forsvar og strategisk kommunikasjon	Styrket militærmakt	Begrense effektene av desinformasjon, fremfor å aktivt motsi eksisterende falske nyheter	Vurdering av sårbarhet i kritisk infrastruktur
Avdekke	Endret etterretningslovgivning (gått vekk fra separat innenlands- og utenlands-innhenting)	Endret etterretningslovgivning, dømt i EMD	Separat innenlands og utenlands etterretning	Endret etterretningslovgivning, dømt i EMD	Endret etterretningslovgivning (fokus cyber- angrep)	Åpenhetsregister for individer og enheter som representerer utenlandske aktører
Håndtering	Kan benytte et bredt spekter av tilgjengelige virkemidler	Benytte politistyrker for å beskytte kritisk infrastruktur	Kan benytte et bredt spekter av tilgjengelige virkemidler	Elastisk kommunikasjon	Kan benytte et bredt spekter av tilgjengelige virkemidler	Terskel for militær respons er uklar, spesielt i det digitale rom og romdomenet

6.1 Vurdering av funn for å styrke samfunnets motstandsdyktighet (avskrekke)

Det gjennomføres og planlegges en rekke tiltak for å avskrekke sammensatte trusler ved å bygge motstandsdyktighet i landene i denne studien. Dette bli sett på som «moderne avskrekking» ifølge forskeren Braw (2018) ved *Royal United Services Institute* (RUSI), og som videre fremheves av professor Gunhild Hoogensen Gjørv *et al.* (2022). For å øke robusthet i befolkningen har flere av landene i denne studien fremhevet behovet for et fritt, mangfoldig, ansvarlig og robust media. Dette blir sett på som en viktig komponent i sikkerhetskonseptet i for eksempel Finland. Australia har spesielt fremhevet kursing i medieforståelse blant unge. Det er likevel verdt å stille spørsmålstegn ved om det er den unge delen av befolkningen som har størst behov for medietrening. En undersøkelse gjort i Norge av Medietilsynet i 2019 fant for eksempel at unge var blant de som er best på å avsløre falske nyheter (Medietilsynet, 2019).

I tillegg bør det fremheves at opplæring av hvordan sosiale medier fungerer kan være komplimenterende til de tradisjonelle mediene, fordi sosiale medier har en plattform som enkelt kan brukes til påvirkningsoperasjoner (Bergh, 2019, 2020). Storbritannia har utviklet et verktøysett som skal kunne bidra til å identifisere desinformasjon. I Finland gjennomføres det også en rekke kurs om sivilt-militært samarbeid med offentlige byråkrater, privat sektor og på universitetet.

Estland, Finland og Sverige har også fremhevet behovet for å lagre mat, drivstoff og utstyr til befolkningen ved en større krise. Denne type beredskapslagring kan sies å i større grad følge en «invasjonstankegang», enn en tanke om svikt i forsyningskjedene, men koronapandemien i 2020–2022 viste at beredskapslagring av varer kan være nødvendig også ved andre typer kriser (NOU 2021: 6). Dette viser likevel til en tankegang der en allerede er høyt på en kriseskala, og vil ikke nødvendigvis være relevant ved situasjoner med lavere intensitet. Vi problematiserer spørsmålet rundt sammensatte trusler i en krisesetting i kapittel 6.3 om vurderingen av funn for å styrke evnen til håndtering.

Som en del av arbeidet med å øke motstandsdyktighet, og med dette bidra til avskrekking ved nektelse, har flere av landene i denne studien fremhevet behovet for å vurdere sårbarheter i infrastrukturen. Kritisk infrastruktur vil ikke bare påvirke statens handlefrihet, men vil i forlengelse også ha en effekt på befolkningens tilgang på tjenester og ressurser. Å identifisere og lukke disse sårbarhetene vil forbli en viktig og kontinuerlig oppgave.

For å se nærmere på hva Norge kan lære vil vi ta utgangspunkt i norsk sikkerhetspolitikk. Norsk sikkerhetspolitikk har lenge vært basert på «balanse mellom avskrekking og beroligelse», hvor avskrekking av fiendtlige aktører skjer gjennom egen militær evne, medlemskap i Nato og avtaler med nære allierte, mens beroligelse av ikke-allierte skjer gjennom dialog, diplomati og åpenhet (Prop. 14 S (2020–2021), s. 22). Ser en på Norges sikkerhetspolitiske forhold til Russland og den store militære asymmetrien mellom de to landene, er norsk Nato-medlemskap og avtaler med nære allierte avgjørende for å oppnå troverdig militær avskrekking. Samtidig må Forsvaret ha en egen evne til avskrekking for å forhindre et *fait accompli* som kan gjøre det vanskeligere å få alliert støtte ved et væpnet angrep på Norge (Diesen, 2021; Guttelvik & Hennum, 2019; Oma,

2021). Det norske forsvarskonseptet er altså basert på vår nasjonale forsvarsevne, kollektiv avskrekking og forsvar gjennom Nato, samt bilaterale planer for støtte og forsterkning fra nære allierte (Prop. 14 S (2020–2021), s. 25–26). Dette forsvarskonseptet understøttes av totalforsvaret (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2018).

Under terskelen for en direkte væpnet konflikt er det totalforsvarsarbeidet, samfunnssikkerhetsarbeidet og det forebyggende sikkerhetsarbeidet etter sikkerhetsloven som danner grunnlaget for å håndtere sammensatte trusler.[17] Både Prop. 14 S (2020–2021) og Meld. St. 5 (2020–2021) fremhever fortsatt styrking av samfunnets motstandsdyktighet. Norge er også et velfungerende demokrati med lav korrupsjon, høy levestandard og høy tillit til myndighetene (FN-sambandet, u.å.; The Economist Intelligence Unit, 2020; Transparency International, 2021). Dette gir et godt utgangspunkt for avskrekking av sammensatte trusler ved nektelse (Wigell, 2021).

I en FFI-studie av utfordringsbildet som de norske politi- og påtaletjenestene står overfor frem mot 2030 fremheves undergraving av demokratiet og sammensatte trusler som svekker tilliten mellom befolkingen og myndighetene som de farligste truslene mot nasjonal sikkerhet under terskelen for væpnet konflikt (Sellevåg *et al.*, 2021). Land som Finland, Sverige og Estland har fokus på psykologisk motstandsdyktighet og psykologisk forsvar mot slike trusler (jf. omtale i kapittel 5). Hvordan står det så til med Norges evne til psykologisk forsvar som en del av avskrekking ved nektelse?

Psykologisk forsvar var ett av fire prinsipielle hovedkrav som Forsvarskommisjonen av 1946 trakk frem som viktige for organiseringen av forsvaret av Norge. «Av grunnleggende betydning er det at det hersker et forhold av gjensidig tillit og respekt mellom forsvarsmakt og folk», skrev Forsvarskommisjonen (1949b, s. 103). Psykologisk krigføring ble da beskrevet på følgende måte: «En mulig angriper vil fra første stund og kanskje alt før et direkte angrep settes inn, søke å redusere vår *vilje* til motstand så langt som han på noen måte kan makte det» (Forsvarskommisjonen, 1949a, s. 62). Denne beskrivelsen av psykologisk krigføring står seg godt også i dag i lys av spredning av desinformasjon på sosiale medier.

Ifølge historiker Magnus Håkenstad (2019, s. 33–34) ble det psykologiske forsvaret senere kalt *informasjonsberedskap*. Informasjonsberedskapen skulle «vedlikeholde forsvarsviljen, forberede befolkningen på hva som vil kreves, og formidle myndighetenes beslutninger. Særlig viktig var det å bekjempe rykter og fiendtlig propaganda» (s. 33). Til tross for dette er ikke begrepene «psykologisk forsvar» eller «forsvarsvilje» eksplisitt omtalt i regjeringens beskrivelse av totalforsvarskonseptet (Forsvarsdepartementet & Justis- og beredskapsdepartementet, 2018) eller i gjeldende samfunnssikkerhetsmelding (Meld. St. 5 (2020–2021)). Selv om norske myndigheter har tatt grep for å motvirke spredning av desinformasjon (Meld. St. 5 (2020–2021), s. 95–101), først og fremst gjennom å styrke evnen til kildekritikk, fremstår ikke politikken like uttrykt som i våre naboland, Sverige og Finland (jf. kapittel 5.2 og 5.2). Dog skal det påpekes at regjeringen

[17] Etterretning er også en del av dette arbeidet, men vi diskuterer etterretning som en del av «situasjonsforståelse» i kapittel 6.2.

har tatt til orde for å styrke kompetansen og fagmiljøet i forsvarssektoren rundt strategisk kommunikasjon, samt integrere strategisk kommunikasjon i operativt planverk og i militære operasjoner (Prop. 14 S (2020–2021), s. 73–74).

Som nevnt i kapittel 5.2, har Sverige nylig opprettet Myndigheten för psykologiskt försvar (2022) hvis formål er å:

> *[…] värna det öppna och demokratiska samhället, den fria åsiktsbildningen samt Sveriges frihet och oberoende.*
>
> *Det psykologiska försvaret ska, både nationellt och internationellt, kunna identifiera, analysera, möta och förebygga otillbörlig informationspåverkan och annan vilseledande information som är riktad mot Sverige eller svenska intressen. Det kan handla om desinformation som syftar till att försvaga landets motståndskraft och befolkningens försvarsvilja eller till att på ett otillbörligt sätt påverka människors uppfattningar, beteenden och beslutsfattande.*
>
> *Det psykologiska försvaret ska även stärka befolkningens förmåga att kunna upptäcka och motstå påverkanskampanjer och desinformation. Därigenom bidrar det psykologiska försvaret till att skapa motståndskraft och försvarsvilja hos befolkningen och i samhället.*
>
> *Myndigheten för psykologiskt försvar ska verka både förebyggande och operativt och ska kunna fullgöra sina uppgifter i fredstid såväl som i krig. Vi ska bidra till ett starkt svenskt totalförsvar som förebygger konflikter och är fredsbevarande.*

I Finland er *psykologisk motstandsdyktighet* en integrert del av den finske, nasjonale sikkerhetsstrategien og gitt en vid betydning (The Security Committee, 2017, s. 22; se også kapittel 5.1):

> *Psychological resilience means the ability of individuals, communities, society and the nation to withstand the pressures arising from crisis situations and to recover from their impacts. Good psychological resilience facilitates the recovery process. Psychological resilience is expressed in the citizens' will to defend their country's independence as well as in the determination to maintain the livelihood and security of the population in all situations. Creating and maintaining psychological resilience is a longstanding and cross-cutting effort involving different administrative branches.*

Videre fremheves det i den finske sikkerhetsstrategien at (The Security Committee, 2017, s. 22):

> *The strength of the nation's psychological resilience strongly depends on how society manages to safeguard vital functions and perform the strategic tasks associated with them. There may be deliberate efforts to weaken the operating capability of the democratic institutions, position of the state leadership and the credibility of decision-makers during a crisis. Citizens' trust in the authorities is essential for maintaining psychological resilience.*

Dette er i tråd med konklusjonene til Rácz (2015, s. 92):

> *Hybrid warfare is built on capitalizing on the weaknesses of a country, on flaws in its political system, administration, economy and society. If an adversary cannot detect sufficient weaknesses, then no full-scale attack can be launched, meaning that hybrid warfare never reaches the second, attack phase.*

Psykologisk forsvar er derfor en viktig del av arbeidet med å styrke samfunnets årvåkenhet og motstandsdyktighet mot sammensatte trusler.

Nå skal det påpekes at tilliten mellom norske myndigheter og befolkningen er høy (OECD, 2021a, s. 207). Det er derfor nødvendigvis ikke slik at det norske samfunnet er spesielt sårbart mot uønsket påvirkning fra fremmedstatlige aktører. Det betyr likevel ikke at dette ikke kan forandre seg. Skal imidlertid psykologisk forsvar fungere som en troverdig avskrekkingsstrategi krever dette en klart kommunisert evne og vilje.

Ser vi videre på avskrekking ved straff, krever dette som nevnt troverdig evne og vilje til å håndtere hendelsene. I hvilken grad Norge kan gjøre nyttiggjøre seg foreslåtte strategier for avskrekking ved straff, vil derfor diskuteres som en del av hvordan Norge kan styrke evnen til håndtering i kapittel 6.3.

6.2 Vurdering av funn for å styrke evnen til situasjonsforståelse (avdekke)

En forutsetning for å klare å avdekke sammensatte trusler er at aktørene har god situasjonsforståelse. Å avdekke trusler og skape situasjonsforståelse henger derfor tydelig sammen. Som fremhevet i Meld. St. 10 (2021–2022), bidrar sammensatte trusler til å «skape dilemma på tvers av sektorielle ansvarsområder, utnytte motpartens sårbarheter og egne muligheter i samspillet mellom sivile og militære aktører og slik viske ut skillet mellom fred og væpnet konflikt». Sammensatte trusler utfordrer derfor situasjonsforståelsen til myndighetene ved at det bidrar til usikkerhet og tvetydighet om hva som er den faktiske situasjonen (Malerud *et al.*, 2021, s. 17). Dette gjør det vanskelig å identifisere truslenes effekt, som igjen påvirker evnen til å iverksette hensiktsmessige mottiltak.

Foreslått mønsterpraksis for Nato og EU og funn fra andre lands tilnærminger fremhever at nasjonal håndtering må være synkronisert, systematisk og tilpasset. Dette fordrer god situasjonsforståelse. Flere land har derfor gjennomført tiltak for å styrke evnen til å etablere situasjonsforståelse (jf. kapittel 5). Som nevnt i kapittel 2, er tilgang på rettidig, relevant informasjon fundamentalt for å kunne oppnå god situasjonsforståelse. Det samme er kompetansen til beslutningstakerne og til analytikerne som analyserer og sammenstiller informasjonen til et beslutningsgrunnlag. Vi har allerede i kapittel 6.1 diskutert de forskjellige kursene og opplæringstilbudene som forskjellige land gjennomfører for å øke motstandsdyktighet, men kursene vil følgelig også bidra til økt situasjonsforståelse. Vi utbroderer ikke videre på disse tiltakene her.

Kompetansen til beslutningstakerne og analytikerne krever at alle partene er enige om hva en står overfor. Som vi forklarte i kapittel 2, omhandler situasjonsforståelse at partene forstår betydningen av situasjonen opp mot egne verdier, målsettinger og kontekst. Det kan derfor være problematisk at begrepsbruken knyttet til sammensatte trusler er så forskjellig. Et gjennomgående tema for flere av landene i denne studien er nemlig at begrepsbruken rundt sammensatte trusler er inkonsekvent både på tvers av landene, men også innad i landene. At en bruker forskjellige begreper for å forklare konseptet «sammensatte trusler» trenger ikke i seg selv å være et problem, men det kan være problematisk om det er usikkerhet tilknyttet hva en faktisk snakker om i prosessen med å utvikle mottiltak.

Det kan derfor være utfordrende å utvikle politikk når bruken av begrepet «sammensatte trusler» ikke skiller mellom forskjellige typer aktiviteter, intensitetsnivå på innblandingen og alvorlighetsgrad. Haga (2021) anbefaler å være tydelig i begrepsbruken og mener det er nyttig å konkretisere trusselen i stedet for å bruke vagere begrep som sammensatte trusler og hybridkrig. For å bidra til mer tydelighet foreslår Wigell *et al.* (2021, s. 11) å skille mellom «hybrid innblanding», «hybride operasjoner» og «hybridkrig». Vi er ikke overbevist om at enda et nytt sett med «hybrid»-begrep vil øke evnen til å forstå hva en står overfor av trusler.

Ved FFI jobber vi med utvikling av et annet type skille enn «hybrid innblanding», «hybride operasjoner» og «hybridkrig» som Wigell *et al.* (2021) har skissert. Vi foreslår heller å tydeliggjøre innholdet til begrepet «sammensatte trusler» gjennom å betrakte hva slags type aktiviteter begrepet består av. Foreløpige resultater basert på morfologisk analyse viser at sammensatte trusler som helhet består av strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt, der handlinger som faller innenfor de fem kategoriene internasjonal politikk, tvangsdiplomati, maktposisjonering, fordekt tvang, samt sabotasje og likvidasjoner, utnyttes for å nå strategiske målsettinger. Å forstå hva slags handlinger en står overfor kan også bidra til relevante mottiltak (Bergaust & Sellevåg, u.å.).

For å øke situasjonsforståelsen i landene som denne studien har tatt for seg, har det blitt opprettet en rekke situasjonssentre og nettverk på tvers av offentlig etater og private aktører, også i samarbeid med universiteter. Hvorvidt dette ledes fra statsministerens kontor eller fra et direktorat er løst på forskjellige måter, men at det er behov for tverrsektoriell situasjonsforståelse fremstår det enighet om. Slike situasjonssentre kan potensielt ha nytte av internasjonalt samarbeid også. Finland og Sverige har blitt anbefalt å se til Norden for totalforsvarssamarbeid, mens Nederland ser spesielt til samarbeid med Storbritannia, EU og Nato. Storbritannia og Australia har

et etablert internasjonalt samarbeid på etterretning gjennom *Five Eyes*, mens de andre landene i denne studien står utenfor.

Flere av landene i denne studien har sett behovet for å oppdatere lovgivning om etterretning i lys av den raske digitale utviklingen. Finland har for eksempel gått vekk fra separat innenlands- og utenlandsinnhenting, og har heller en sivil og en militær etterretningsenhet. I tillegg har Finland styrket overvåkning av oppkjøp av eiendom og land. Nederland og Australia har også enheter som innhenter informasjon både innenfor og utenfor landegrensene. Likevel har ikke alle landene kun hatt suksess med de nye måtene å innhente informasjon på, og både Sverige og Storbritannia har blitt dømt i EMD på grunn av måten de har forsøkt å innhente informasjon. Disse dommene fremhever noe av problematikken forbundet med informasjonsinnhenting i stor skala. Det skal fremheves at enkelte norske forskere har stilt spørsmålstegn ved om dagens innretning av etterretningstjenestene i Norge er hensiktsmessig (Friis & Hansen, 2020). Dette er fordi dagens trusler ikke stopper på grensen og «nær sagt alle dagens trusler har forankringer både innenlands og utenlands samtidig» (Friis & Hansen, 2020, s. 183).

Et annet type tiltak for å øke situasjonsforståelse er Australias forsøk på å tvinge frem aktører til åpenhet gjennom rapporteringsforpliktelser. Dette gjøres ved et åpenhetsregister. Tanken bak et slikt smalt juridisk tiltak er å sørge for at tiltaket som innføres ikke skal gå på bekostning av verdiene de forsøker å beskytte. Selv om tiltak for å fremme åpenhet og tiltak for å øke situasjonsforståelse gjennom etterretning er kvalitativt forskjellige, er begge eksempler på hvordan situasjonsforståelse kan oppnås.

For å øke oppmerksomheten rundt sammensatte trusler har både Sverige og Finland opprettet en såkalt «hybrid-ambassadør»-stilling. Det er uklart for oss om slike stillinger kan bidra til internasjonalt samarbeid som igjen kan bidra til gode og effektive tiltak mot sammensatte trusler – spesielt sammenlignet med andre etablerte diplomatiske mekanismer.

Situasjonsforståelsen for truslene en står overfor vil også være preget av klimaendringene, samt sekundæreffektene det vil medføre. Forsvarsdepartementet beskrev i Langtidsplan for forsvarssektoren at klimaendringene er en «trusselmultiplikator» (Prop. 14 S (2020–2021), s. 42). Risiko for sosial og økonomisk uro på grunn av klimaendringer er påpekt av blant annet *Stockholm International Peace Research Institute* (SIPRI), FNs miljøprogram (UNEP) og Lausund *et al.* (2022) (Hegazi & Seyuba, 2022; Mobjörk *et al.*, 2020; UNEP & EU, 2022). Med en lang tidshorisont kan en ikke utelukke at denne sosiale uroen kan bli utnyttet til å skape ytterligere splid i samfunnet gjennom for eksempel påvirkningsoperasjoner. Sammensatte trusler bør derfor sees i lys av klimaendringene, i tillegg til tilpasning og tiltak for å begrense disse. Vi viser til separat delutredning for Forsvarskommisjonen om klima og sikkerhet for mer informasjon om konsekvenser av klimaendringer og klimatilpasninger for Forsvaret frem mot 2040 (Lausund *et al.*, 2022).

6.3 Vurdering av funn for å styrke evnen til håndtering (respons)

I det gjeldende sikkerhetspolitiske utfordringsbildet må norske myndigheter være forberedt på å håndtere situasjoner hvor en fremmed stat benytter sammensatte trusler for å sette Norge under press. Uten tilstrekkelig evne til avskrekking, krisehåndtering og respons kan slike situasjoner skje hyppigere (Skjelland *et al.*, 2022, s. 51). Skal straffereaksjoner og andre håndteringsmulighetene være troverdige og effektive, må de derimot planlegges, koordineres og samordnes. Dette krever et definert og regulert gjennomføringsansvar (Skjelland *et al.*, 2022, s. 53). Videre må utvikling av straffereaksjoner mot sammensatte trusler ha forankring i folkeretten. Foreslått mønsterpraksis for Nato og EU peker også på at responsen må være aktør-spesifikk og riktig justert for å unngå uønsket eskalering. Imidlertid hevder enkelte norske forskere at Norge har en lang vei å gå når det gjelder strategisk kommunikasjon overfor fremmedstatlige aktører og evne til tverrsektoriell situasjonsforståelse og håndtering (Malerud *et al.*, 2021; Oma, 2021).

Hvordan stater skal kunne respondere, dersom det i det hele tatt gjøres, er komplisert av flere grunner. Én av disse grunnene er at demokratiske rettsstater ikke nødvendigvis kan svare på samme måte som en har blitt rammet av handlinger selv. Som Diesen (2018, s. 26) påpeker, kan ikke Norge eller andre liberale demokratier ta i bruk samme type virkemidler «[g]itt irregulære virkemidlers fordekte og illegitime karakter». Salisbury-forgiftningen i Storbritannia er et godt eksempel på asymmetrisk håndtering, hvor reaksjonen på handlingen var å attribuere og kommunisere åpent, noe som er en betydelig mildere reaksjon enn handlingen i seg selv.

I tillegg kan det være usikkerhet knyttet til om handlinger blir gjennomført i kombinasjon for å skape en forsterkende effekt (jf. figur 4.1). Dersom det er en sammenheng mellom handlingene kan det potensielt senke terskelen for hendelseshåndtering sammenlignet med når handlingene gjennomføres uten sammenheng. I det sistnevnte tilfellet kan terskelen for respons muligens bli for høy.[18] I den forbindelse er det ikke nødvendigvis nyttig å se på sammensatte trusler som et konsept som er begrenset til kombinasjoner av handlinger som brukes strategisk for å oppnå forsterkende effekt. Det kan kanskje vel så godt beskrive hvilke uønskede handlinger som gjennomføres av fremmedstatlige aktører som er uakseptable for Norge og dermed åpner for en motreaksjon. Det er med andre ord enkelte handlinger som krever håndtering også når de gjennomføres tilsynelatende separat fra alt annet.

Dyndal og Larssen (2020, s. 23) skriver at det er «flytende overganger mellom hendelser og episoder, kriser og sikkerhetspolitiske kriser, og til sist krig». Dette kan gjøre håndteringen vanskelig. At handlinger kan skje uten at det nødvendigvis har blitt erklært krise, og en påfølgende krisestab blir etablert, er sammensatte trusler-problematikken er godt eksempel på. I motsetning til store hendelser som skjer sjeldent, kan sammensatte trusler bli sett på som små hendelser som heller skjer ofte, men har tilsynelatende liten effekt hver for seg. Den lille effekten kan derfor være desto vanskeligere å avdekke og håndtere. Cullen og Reichborn-Kjennerud (2017, s. 15) kaller hybridkrig for «*death by a thousand cuts*», og det er et godt bilde på hvordan sammen-

[18] FFI skal i perioden 2023–2025 gjennomføre et phd-prosjekt som handler om legitimitet tilknyttet spørsmål om besvarelse av informasjonspåvirkning i sosiale medier.

satte trusler kan forstås som en motsetning til større, men sjeldne, kriser. Samtidig kan en benytte samme type virkemidler som omfattes av begrepet «sammensatte trusler» i en krise eller mellomstatlig konflikt (for sistnevnte, se Diesen, 2018).

Hendelseshåndtering behøver heller ikke være direkte respons på aktøren som gjennomfører handlingen. Håndtering kan også omfatte ekstra sikring av infrastruktur, eller andre kritiske funksjoner, slik som Sverige har fremhevet som et forslag. Dette er foreslått som relevant under høynet beredskap, krig eller såkalte hybride situasjoner, men som tidligere nevnt er dette en type tankegang som tilhører høyere opp i krisespekteret. Slike tiltak krever naturligvis at det på forhånd har blitt avklart hva som skal beskyttes og at det her er tydelige målsettinger, samt tydelig synkronisert og koordinert nasjonal håndtering.

Det har blitt poengtert i kapittelet om foreslått mønsterpraksis i EU (kapittel 4.2), at eierskap til håndtering og respons på sammensatte trusler faller på statlige myndigheter. Imidlertid bør det utøves aktsomhet hvis Forsvaret skal bistå politiet med håndtering av eksempelvis sivile ordensforstyrrelser og opptøyer for å opprettholde ro og orden. Det er politiet som er instansen som bekrefter og sikrer borgernes rettssikkerhet gjennom forebyggende, håndhevende og hjelpende virksomhet (Finstad, 2018).

Det bør også vurderes hvordan internasjonalt samarbeid kan påvirke og eventuelt bidra til bedre håndtering, og ikke bare evnen til situasjonsforståelse (avdekke) og motstandsdyktighet (avskrekke).

7 Anbefalinger til Forsvarskommisjonen

I denne studien har FFI sett nærmere på hvordan andre land jobber for å motvirke sammensatte trusler og hva Norge eventuelt kan lære av dette. På bakgrunn av foreslått mønsterpraksis for Nato og EU og erfaringer fra Finland, Sverige, Estland, Storbritannia, Nederland og Australia, presenterer FFI her sine anbefalinger til Forsvarskommisjonen.

7.1 Anbefalinger for å styrke motstandsdyktighet (avskrekke)

Det største handlingsrommet Norge har som et liberalt demokrati er å styrke motstandsdyktigheten i vårt demokrati, til kritiske samfunnsfunksjoner og i befolkningen. Viktige tiltak her er å lukke sårbarheter i kritiske samfunnsfunksjoner, infrastruktur og forsyningskjeder, etablering av beredskapslagre og styrke den psykologiske motstandsdyktigheten i befolkningen (jf. kapittel 6.1). Basert på foreslått mønsterpraksis for Nato og EU, samt andre lands tilnærminger, *vurderer FFI at psykologisk forsvar er like viktig i dag som det var etter andre verdenskrig, men det må innrettes for vårt moderne samfunn*. Foreslått mønsterpraksis for Nato og EU tilsier at økt medieforståelse i befolkningen og kunnskap om hvilke verdier som skal beskyttes forblir nødvendig. Det samme er å sikre frie, mangfoldige og ansvarlige medier. *FFI anbefaler at Forsvarskommisjonen vurderer hvordan et moderne psykologisk forsvar kan innrettes i Norge*.

Forsvarets viktigste oppgaver under terskelen for direkte væpnet konflikt vil være å opprettholde evne til militær avskrekking sammen med Nato og nære allierte, bidra med etterretning, samt å ha situasjonsforståelse i domener hvor Forsvaret har unike kapasiteter. *Det er behov for mer kunnskap om Norges handlingsrom for bruk av straff i et avskrekkingsperspektiv.*

Forsvaret kan også spille en viktig rolle med å bistå sivile myndigheter med å ivareta samfunnssikkerheten, eksempelvis med sikring av kritisk infrastruktur og kritiske samfunnsfunksjoner (jf. kapittel 6.1). Det er likevel poengtert av flere aktører i denne studien at tiltak må utvikles på en måte som ikke går på bekostning av de verdiene man forsøker å beskytte. Det er derfor viktig å se på de potensielle konsekvensene av en utvidelse av Forsvarets ansvar. Dersom Forsvarets ansvar tilknyttet avskrekking, avdekking og håndtering av sammensatte trusler skal utvides, må dette vurderes nøye. *FFI anbefaler at det utøves aktsomhet ved mulige utvidelser av Forsvarets ansvar knyttet til å avskrekke, avdekke og håndtere sammensatte trusler.*

7.2 Anbefalinger for å styrke evnen til situasjonsforståelse (avdekke)

Som illustrert gjennom forslag til mønsterpraksis og de forskjellige landenes tilnærming til sammensatte trusler er det ikke enighet om hva «sammensatte trusler» omfatter. Imidlertid er en enighet om begrepsbruk og -forståelse avgjørende for god situasjonsforståelse (jf. kapittel 6.2). *FFI anbefaler at Forsvarskommisjonen tar utgangspunkt i Forsvarsdepartementets definisjon av sammensatte trusler slik den er gitt i Meld. St. 10 (2021–2022) (s. 15)*, i sin vurdering av potensielle sikkerhets- og forsvarspolitiske veivalg og prioriteringer Norge kan ta for å ivareta

norsk sikkerhet i møtet med sammensatte trusler på best mulig vis. FFI vurderer at denne definisjonen i hovedsak er i samsvar med foreslått mønsterpraksis for Nato og EU samt akademisk litteratur.

Flere land har gjennomført tiltak og etablert situasjonssentre for å styrke regjeringens situasjonsforståelse (jf. kapittel 6.2). Hvorvidt dette ledes fra statsministerens kontor eller fra et direktorat er løst på forskjellige måter. I denne rapporten tar ikke FFI stilling til hvordan dette bør løses for norske forhold, men påpeker behovet for tverrsektoriell situasjonsforståelse for at en evner å avdekke sammensatte trusler og finne riktig håndtering. Tilgang på rettidig, relevant informasjon er fundamentalt for å kunne oppnå god situasjonsforståelse. Det samme er kompetansen til beslutningstakerne og til analytikerne som analyserer og sammenstiller informasjonen til et beslutningsgrunnlag. *FFI anbefaler at Forsvarskommisjonen vurderer hvordan en strategisk funksjon for å styrke regjeringens situasjonsforståelse kan innrettes.*

Flere land har styrket sine etterretningstjenesters evne til å avdekke sammensatte trusler og endret etterretningslovgivningen (jf. kapittel 6.2). Særlig Finland har gjort store endringer ved å gå bort fra separat innenlands- og utenlandsinnhenting og over til én sivil og én militær etterretningsenhet (jf. kapittel 5.1). Ifølge den finske regjeringen har dette ført at den nasjonale sikkerhetssituasjonen har blitt forbedret. En vurdering av i hvilken grad de finske endringene vil være nyttige for Norge, vil kreve en mer inngående utredning enn hva som har vært mulig i denne rapporten. *FFI anbefaler at Forsvarskommisjonen vurderer hvordan norske etterretnings- og sikkerhetstjenester kan styrkes og om det er behov for å gjøre endringer i dagens struktur for innenlands- og utenlandsetterretning.*

En tydelig forståelse av hva slags handlinger en står overfor er en forutsetning for å identifisere mottiltak og deretter identifisere ulike aktørers rolle, inkludert hvilke oppgaver Forsvarets skal utføre. Denne studien har vist at det er tidvis er utydelig hva som legges i begrepet «sammensatte trusler» (jf. kapittel 6.2). Det vil bidra til mer klarhet dersom eksempelvis cyberoperasjoner blir kalt «cyberoperasjoner» og sabotasje blir omtalt som «sabotasje» i stedet for vagere ord som «hybridangrep» eller liknende uttrykk. Kunnskap om hvordan sammensatte trusler bør møtes må derfor videreutvikles i takt med det sikkerhetspolitiske utfordringsbildet og hvordan samfunnet endrer seg. *FFI anbefaler at forståelsen av sammensatte trusler videreutvikles fordi det er utfordrende å utvikle politikk når begrepsbruken ikke skiller mellom forskjellige typer aktiviteter, intensitetsnivå på innblandingen og alvorlighetsgrad.*

7.3 Anbefalinger for å styrke evnen til håndtering (respons)

Foreslått mønsterpraksis for Nato og EU, samt funn fra andre lands tilnærminger fremhever at nasjonal håndtering må være synkronisert, systematisk og tilpasset (jf. kapittel 6.3). Håndteringen av Salisbury-hendelsen i Storbritannia er et eksempel på en slik tilpasset og synkronisert tilnærming. Dette krever god tverrsektoriell situasjonsforståelse. Det er vesentlig at de som har eierskap til de forskjellige sektorene/domenene samvirker når uønskede handlinger finner sted i flere sektorer og/eller domener samtidig. Samarbeid på tvers av sivile og militære aktører i det

offentlige Norge, samt med sivilsamfunnet, akademia og privat næringsliv kan bidra til økt situasjonsforståelse. *FFI anbefaler at Forsvarskommisjonen vurderer hvordan nasjonal håndtering av sammensatte trusler kan gjøres synkronisert, systematisk og tilpasset.*

FFI anbefaler at Forsvarskommisjonen ser nærmere på hvordan en kan innrette en helhetlig og proaktiv samfunnstilnærming med evne til å koordinere håndtering på tvers av aktører i det som i dag omtales som totalforsvaret (jf. kapittel 6.3). Dette vil trolig kreve at reaktive, hendelsesdrevne tilnærminger erstattes av strategisk sivil forsvarsplanlegging slik svenske forskere har foreslått (Lindgren & Ödlund, 2017). Betydningen av å forstå fremmedstatlige aktørers sikkerhetspolitikk og strategiske kultur vil være nødvendig for å skreddersy en effektiv avskrekkingsstrategi mot sammensatte trusler. *FFI anbefaler at Forsvarskommisjonen vurderer et helhetlig nasjonalt forsvars- og sikkerhetskonsept nærmere.*

For å ivareta rettssikkerhet, demokrati og menneskerettigheter bør tiltak vurderes å være smale for å unngå at tiltakene en igangsetter går på bekostning av verdiene en forsøker å beskytte (jf. kapittel 6.3). For å oppnå dette kan da være relevant å tenke bredere enn statssikkerhet ved å også omfatte individets sikkerhet og rettigheter i utformingen av mottiltak. Tiltak som rammer smalt vil i mindre grad ha utilsiktede konsekvenser. Åpenhetstiltak vil i mindre grad gå på bekostning av rettssikkerhet, demokrati og menneskerettigheter. *FFI anbefaler at Forsvarskommisjonen ser nærmere på tiltak som fremmer åpenhet.*

Referanser

AIVD. (2018). *AIVD Annual Report 2018*. Ministry of the Interior and Kingdom Relations. https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018.

AIVD. (u.å.-a). *The AIVD's role in national security*. General Intelligence and Security Service, Ministry of the Interior and Kingdom Relations. Hentet 20. september 2022 fra https://english.aivd.nl/about-aivd/the-aivd%E2%80%99s-role-in-national-security.

AIVD. (u.å.-b). *Tasks and areas of interest*. General Intelligence and Security Service, Minstry of the Interior and Kingdom Relations. Hentet 20. september 2022 fra https://english.aivd.nl/about-aivd/tasks-and-areas-of-interest.

Alperovitch, D. (2018, 28 January). Stopping the Next Cyber Conflict. *The Cipher Brief*. https://www.thecipherbrief.com/column_article/stopping-next-cyber-conflict.

ASIS. (u.å.). *ASIS operates collaboratively within Australia's National Intelligence Community.* Hentet 20. september 2022 fra https://www.asis.gov.au/About-Us/Governance/National-Intelligence/.

Balcaen, P., Bois, C. D. & Buts, C. (2021). A Game-theoretic Analysis of Hybrid Threats. *Defence and Peace Economics*, 1-16. https://doi.org/10.1080/10242694.2021.1875289.

Barber, N. (2017). A warning from the Crimea: hybrid warfare and hte challenge for the ADF. *Australian Defence Force Journal*, (No. 201), 46-58. https://search.informit.org/doi/pdf/10.3316/ielapa.812433256559972.

BBC News. (2018, 4. oktober 2018). How the Dutch foiled Russian 'cyber-attack' on OPCW. *BBC News*. https://www.bbc.com/news/world-europe-45747472.

Bergaust, J. C. & Sellevåg, S. R. (u.å.). Dissecting and revising: An improved conceptualisation of hybrid interference (vitenskapelig artikkel under utarbeidelse).

Bergh, A. (2019). *Social network centric warfare – understanding influence operations in social media* (FFI-rapport 19/01194). Forsvarets forskningsinstitutt.

Bergh, A. (2020). *Påvirkningsoperasjoner i sosiale medier – oversikt og utfordringer* (FFI-rapport 20/01694). Forsvarets forskningsinstitutt.

Brânda, O. & Saulic, A. (2020). Hybrid Threats on Nato's Eastern Flank- A Comparative Analysis. *International Conference Knowledge-Based Organization 26*(1), 33-41. https://doi.org/10.2478/kbo-2020-0005.

Braw, E. (2018, 10. oktober 2022). Modern Deterrence: Preparing for the Age of Grey-Zone Warfare. *RUSI*. https://rusi.org/explore-our-research/publications/rusi-newsbrief/modern-deterrence-preparing-age-grey-zone-warfare.

Buchanan, E. (2019). *Hybrid warfare: Australia's (not so) new normal*. Australian Strategic Policy Institute (ASPI). Hentet 15. september 2022 fra https://www.aspistrategist.org.au/hybrid-warfare-australias-not-so-new-normal/.

Chana, D. (2021). *The future of policing in the face of emerging and disruptive technologies - A report prepared for FFI*.

CSIS. (n.d.). *China Island Tracker*. Center for Strategic & International Studies.

Cullen, P. J. & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. A Multinational Capability Development Campaign project*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Den Europeiske Union. (2016). *Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats a European Union response* (JOIN/2016/018 final). High Representative of the Union for Foreign Affairs and Security Policy. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

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

Diesen, S. (2021). *Avskrekking og beroligelse – en kritisk militærfaglig betraktning* (IFS Insights 6/2021). Institutt for forsvarsstudier.

Dyndal, G. L. & Larssen, A.-K. (2020). Innledning. I G. L. Dyndal & A.-K. Larssen (Red.), *Strategisk ledelse i krise og krig – det norske systemet* (s. 21–34). Universitetsforlaget.

Egloff, F. J. (2020). Public attribution of cyber intrusions. *Journal of Cybersecurity*, *6*(1), tyaa012. https://doi.org/10.1093/cybsec/tyaa012.

Egloff, F. J. & Smeets, M. (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*, 1-32. https://doi.org/10.1080/01402390.2021.1895117.

Ellehuus, R. (2020, 03.10.22). Strange Birds in the Archipelago: Finland's Legislation on Foreign Real Estate Investment. *CSIC.org*. https://www.csis.org/blogs/kremlin-playbook-spotlight/strange-birds-archipelago-finlands-legislation-foreign-real-estate.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, *37*(1), 32-64. https://doi.org/10.1518/001872095779049543.

Estonian Foregin Intelligence Service. (2022). *International Security and Estonia*. Estonian Foregin Intelligence Service. Government. https://raport.valisluureamet.ee/assets/VLA_report_2022_ENG.pdf.

Estonian Foreign Intelligence Service. (u.å.). *Estonian Foreign Intelligence Service public report 2022*. Hentet 17. oktober 2022 fra https://www.valisluureamet.ee/en.html.

Etterretningstjenesten. (2022). *Fokus 2022. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*.

Ferm, T., Eronen, P., Nevaste, N., Olkkonen, I., Puistola, J.-A., Toverød, N., Hennum, A. C., Malerud, S. & Fridheim, H. (2018). *A description of two national conceptual approaches for establishing Hybrid Threat/ Hybrid Influence Situational Awareness*. Forsvarets forskningsinstitutt.

Finstad, L. (2018). *Hva er politi* (Bd. 1. utgave). Universitetsforlaget.

FN-sambandet. (u.å.). *HDI - indeks for menneskelig utvikling*. Hentet 4. november 2022 fra https://www.fn.no/Statistikk/hdi-menneskelig-utvikling.

Forsvarsdepartementet & Justis- og beredskapsdepartementet. (2018). *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag*. https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/stotte-og-samarbeid-en-beskrivelse-av-totalforsvaret-i-da.pdf.

Forsvarsdepartementet (Australia). (2020). *2020 Defence Strategic Update*. Forsvarsdepartementet. https://www.defence.gov.au/about/strategic-planning/2020-defence-strategic-update.

Forsvarsdepartementet (Estland). (2011). *National Defence Strategy*. Forsvarsdepartementet. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf.

Forsvarsdepartementet (Estland). (2021). *The Estonian Foreign Intelligence Service has published a report on external security threats*. Forsvarsdepartementet (Estland). Hentet 05.10.22 fra https://kaitseministeerium.ee/en/news/estonian-foreign-intelligence-service-has-published-report-external-security-threats.

Forsvarsdepartementet (Estland). (u.å.). *Estonian National Defence 2022*. Kaitseministeerium. https://www.kaitseministeerium.ee/riigikaitse2022/index-en.html.

Forsvarsdepartementet (Nederland). (2019). *Annual report Nethelands Defence Intelligence and Security Service 2019*. Ministry of Defence. https://english.defensie.nl/downloads/annual-reports/2020/04/30/annual-report-nld-diss-2019.

Forsvarsdepartementet (Nederland). (2022). *A Stronger Netherlands, A Safer Europe: Investing in a Robust NATO and EU*. Ministry of Defence. https://english.defensie.nl/downloads/publications/2022/07/19/defence-white-paper-2022.

Forsvarsdepartementet (Nederland) og Utenriksdepartementet (Nederland). (2022). *Adviesaanvraag over hybride dreigingen [Forespørsel om råd om hybride trusler]*. Forsvarsdepartementet & Utenriksdepartementet. Regjeringen (Nederland). https://www.rijksoverheid.nl/documenten/brieven/2022/07/08/adviesaanvraag-inzake-hybride-dreigingen.

Forsvarskommisjonen. (1949a). *Innstilling fra Forsvarskommisjonen av 1946 : Del 1: Grunnleggende synspunkter og forslag*. https://urn.nb.no/URN:NBN:no-nb_digibok_2007020101104.

Forsvarskommisjonen. (1949b). *Innstilling fra Forsvarskommisjonen av 1946 : Del 2: Rekruttering av personell til landets samlede forsvar ; Del 5: Forsvarets sivile hovedsektor ; Del 6: Særlige spørsmål*. Elektronisk reproduksjon [Norge] Nasjonalbiblioteket Digital 2017-06-15. https://urn.nb.no/URN:NBN:no-nb_digibok_2017061507327.

Forsvarskommisjonen. (u.å.). *Mandat*. Hentet 2. november 2022 fra https://forsvarskommisjonen.no/mandat/.

Forsvarskommisjonen (Sverige). (2017). *Resilience - the total defence concept and the development of civil defence 2021-2025*. Ministry of Defence. https://www.government.se/press-releases/2017/12/swedish-defence-commission-presents-report-on-total-defence-concept-and-civil-defence/.

Forsvarskommisjonen (Sverige). (2019). *The Swedish Defence Commission's white book on Sweden's Security Policy and the Development of the Military Defence 2021-2025*. Ministry of Defence. https://www.government.se/4ada4f/globalassets/government/dokument/forsvarsdepartementet/forsvarsberedningen/defence-commissions-white-book-english-summary.pdf.

Friis, K. & Hansen, V. V. (2020). Etterretningstjenestene og det nye trusselbildet: Er de beredt? I A. K. Larssen & G. L. Dyndal (Red.), *Strategisk ledelse i krise og krig. Det norske systemet* (s. 183– 195). Universitetsforlaget.

George, A. L. & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Belfer Center for Science and International Affairs, John F. Kennendy School of Government, Harvard University.

Gerring, J. (2017). *Caes Study Research - Principles and Practices* (Second Edition. utg.). Cambridge University Press.

Gjesvik, L. & Øverbø, E. J. (2019). Avskrekke hvem? Betydningen av strategisk kultur for cybersikkerhet. *Internasjonal Politikk*, *77*, 278-287.

Gotkowska, J. (2021). *Sweden's security: the long way towards total defence* (Point of View, Issue. OSW Centre for Eastern Studies. https://www.osw.waw.pl/sites/default/files/PV_Swedens-security_net.pdf.

Grand Chamber ECtHR. (2021a). *Case of Big Brother Watch and Others v. The United Kingdom* European Court of Human Rights (ECtHR),.https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-210077%22]}.

Grand Chamber ECtHR. (2021b). *Case of Centrum för Rettvisa v. Sweden* European Court of Human Rights (ECtHR). https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22respondent%22:[%22SWE%22],%22documentcollectionid2%22:[%22JUDGMENTS%22],%22kpdate%22:[%222017-09-26T00:00:00.0Z%22,%222022-09-26T00:00:00.0Z%22],%22itemid%22:[%22001-210078%22]}.

Guilfoyle, D. & Chan, E. S. Y. (2022). Lawships or warships? Coast guards as agents of (in)stability in the Pacific and South and East China Sea. *Marine policy*, *140*, 105048. https://doi.org/10.1016/j.marpol.2022.105048.

Gjørv, G. H, Gjørv, J., Karlsson, Ø. K., Aasen, M., Rongved, G. F. (2022). De siviles rolle i sammensatt krigføring. I G. F. Rongved & P. M. Norheim-Martinsen (Red.), *Totalforsvaret i praksis* (s. 93-106). Gyldendal Forlag.

Guttelvik, M. S. & Hennum, A. C. (2019). *Prinsipper for norsk avskrekking – en operasjonsanalytisk tilnærming* (FFI-rapport 10/00403). Forsvarets forskningsinstitutt.

Haga, L. P. (2021). Hvordan spiser man en elefant? Hybridkrig og hybride metoder. I A.-K. Larssen (Red.), *Beredskap og krisehåndtering: Utfordringer på sentralt, regional og lokalt nivå* (s. 46–60). Cappelen Damm Akademisk.

Hegazi, F. & Seyuba, K. (2022). *The Social Side of Climate Change Adaptation: Reducing Conflict Risk*. Stockholm International Peace Research Institute (SIPRI). https://sipri.org/publications/2022/sipri-policy-briefs/social-side-climate-change-adaptation-reducing-conflict-risk.

Higgins, A. (2018, 1. november 2018). Finnish soldiers find 'secret Russian military bases' after raiding mysterious island. *The Independent*. https://www.independent.co.uk/news/world/europe/finland-russia-military-bases-sakkiluoto-putin-dmitry-medvedev-police-a8612161.html.

Hjorth, C. B. (2022). *Derfor sender Sverige styrker til Gotland*. Norges Forsvarsforening (NFF). Hentet 17. oktober 2022 fra https://www.forsvarsforeningen.no/nyheter/derfor-sender-sverige-styrker-til-gotland/.

Hoffman, F. G. (2009). *Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict* (Stratgic Forum, Issue. National Defense University. https://www.files.ethz.ch/isn/98862/SF240.pdf.

Hutchens, G. (2018, 28. juni 2018). Sweeping foreign interference and spying laws pass Senate. *The Guardian*. https://www.theguardian.com/australia-news/2018/jun/29/sweeping-foreign-interference-and-spying-laws-pass-senate.

Håkenstad, M. (2019). Den væpnede dugnaden – totalforsvaret under den kalde krigen. I P. M. Norheim-Martinsen (Red.), *Det nye totalforsvaret* (s. 25–40). Gyldendal.

Innenriksdepartementet (Finland). (u.å.). *Civilian intelligence protects Finland's national security*. Hentet 19. september 2022 fra https://intermin.fi/en/national-security/civilian-intelligence.

Jacobs, D. J. (2005). *New Netherland: A Dutch Colony in Seventeenth-Century America*. Brill.

Jalali, S. & Wohlin, C. (2012, 20-21 Sept. 2012). Systematic literature studies: Database searches vs. backward snowballing. Proceedings of the 2012 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement.

Janičatová, S. & Mlejnková, P. (2021). The ambiguity of hybrid warfare: A qualitative content analysis of the United Kingdom's political–military discourse on Russia's hostile activities. *Contemporary Security Policy*, *42*, 312-344.

Jasper, S. (2015). Deterring Malicious Behavior in Cyberspace. *Strategic Studies Quarterly*, *9*(1), 60-85. http://www.jstor.org/stable/26270834.

Jonsson, D., Ingemarsdotter, J., Johansson, B., Rossbach, N., Wedebrand, C. & Eriksson, C. (2019). *Civilt försvar i gråzon*. Totalförsvarets forskningsinstitut. https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4769--SE.

Justis- og beredskapsdepartementet. (2019). *Lov om nasjonal sikkerhet (sikkerhetsloven)*. https://lovdata.no/dokument/NL/lov/2018-06-01-24.

Justis- og beredskapsdepartementet, Helse- og omsorgsdepartementet & Forsvarsdepartementet. (2016). *Nasjonal strategi for CBRNE-beredskap 2016–2020*.

Juurvee, I. & Arold, U. (2021). Psychological Defence and Cyber Security: Two Integral Parts of Estonias Comprehensive Ap-proach for countering Hybrid Threats. *ICONO 14*, *14*(19), 70-94. https://doi.org/10.7195/ri14.v19i1.1628.

Juurvee, I. & Mattiisen, M. (2020). *The Bronze Soldier Crisis of 2007. Revisiting an early case of hybrid Conflict. International Centre for Defence and Security*. Internatioanl Centre for Defence and Security (RKK, ICDS). https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf.

Kaitsepolitseiamet. (u.å.). *Counterintelligence and foreign influence activities*. Hentet 17. oktober 2022 fra https://kapo.ee/en/content/counterintelligence-and-foreign-influence-activities/.

Karlsen, J. (2022). *Klar til å kjempe for hjemlandet*. Forsvaret. Hentet 17. oktober 2022 fra https://www.forsvaret.no/heimevernet/aktuelt/klar-til-a-kjempe-for-hjemlandet.

Kersanskas, V. (2020). *Deterrence: Proposing a more strategic approach to countering hybrid threats* (Hybrid CoE Paper 2). The European Centre of Excellence for Countering Hybrid Threats.

Kristersson, U. (2022, 18. oktober). *Regeringsförklaringen den 18 oktober 2022*. Hentet 3. november 2022 fra https://www.regeringen.se/tal/2022/10/regeringsforklaringen-den-18-oktober-2022/.

Kristiansen, H. & Hoem, N. (2019). Avskrekking som element i cybersikkerhetsstrategi fra et småstatsperspektiv. *Internasjonal Politikk*, *77*(3), 252-265. https://doi.org/http://dx.doi.org/10.23865/intpol.v77.1385.

Lausund, K. B., Granlund, C., Pedersen, M. N., Klepper, K., Gohli, J., Åtland, K., Disen, S., Lausund, R. & Voie, Ø. A. (2022). *Delutredning: Konsekvenser av klimaendringer og klimatilpasninger for forsvaret frem mot 2040* (FFI-rapport under utarbeidelse). Forsvarets forskningsinstitutt.

Lindgren, F. & Ödlund, A. (2017). *Total Defence at the Crossroads* (Offprint from Strategic Outlook 7, Issue. Totalförsvarets forskningsinstitut. https://sldinfo.com/wp-content/uploads/2018/12/http___webbrapp.ptn_.foi_.se_pdf_cb1cc21f-26c9-4738-a70f-9c81b92c0744.pdf.

Lohse, M. (2020a). Finnish Defence Intelligence Agency - an Actor in National Security? *Journal of Strategic Security*, *13*(2), 107-120. https://www.jstor.org/stable/26918088.

Lohse, M. (2020b). The Intelligence Process in Finland. *Scandinavian Journal of Military Studies*, *3*(1), 68-79. https://doi.org/10.31374/sjms.55.

Lohse, M. (2020c). Sharing national security information in Finland. *Information & Communications Technology Law*, *29*(3), 279-290. https://doi.org/10.1080/13600834.2020.1759277.

Löjdquist, F. (2019, 6.09.19). An Ambassador for Countering Hybrid Threats. *RUSI*. https://rusi.org/explore-our-research/publications/commentary/ambassador-countering-hybrid-threats.

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

Mansted, K. (2021). *The Domestic Security Grey Zone: Navigating the Space between Foreign Influence and Foreign Interference* (Occasional Paper, Issue. National Security College, The Australian National University. https://nsc.crawford.anu.edu.au/sites/default/files/uploads/nsc_crawford_anu_edu_au/2021-02/nsc_foreign_interference_op_2021.pdf.

Maskaliunate, A. (2020). Editorial Introduction: Special Issue on Understanding of Total Defence in the Baltic Countries. *Journal on Baltic Security*, *6*(2), 1-2. https://doi.org/https://doi.org/10.2478/jobs-2020-0001.

Medietilsynet. (2019). *Kritisk medieforståelse i den norske befolkningen: En undersøkelse fra Medietilsynet*. Medietilsynet. https://www.medietilsynet.no/globalassets/dokumenter/rapporter/kritisk-medieforstaelse-undersokelser-2019-2020/2019-Kritisk-medieforstaelse-rapport.

Meld. St. 5 (2020-2021). *Samfunnssikkerhet i en usikker verden*. Justis- og beredskapsdepartementet.

Meld. St. 10. ((2021–2022)). *Prioriterte endringer, status og tiltak i forsvarssektoren*. Forsvarsdepartementet.

Meld. St. 10 (2021–2022). *Prioriterte endringer, status og tiltak i forsvarssektoren*. Forsvarsdepartementet.

Mobjörk, M., Krampe, F. & Tarif, K. (2020). *Pathways of Climate Insecurity: Guidance for Policymakers*. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/publications/2020/sipri-policy-briefs/pathways-climate-insecurity-guidance-policymakers.

Monaghan, S. (2022). *Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice* (Hybrid CoE Paper 12). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331-Hybrid-CoE-Paper-12-Fifth-wave-of-deterrence-WEB.pdf.

Monaghan, S., Cullen, P. J. & Wegge, N. (2019). *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Morgan, P. M. (1977). *Deterrence: A Conceptual Analysis*. Sage Publications.

MSB. (2018). *Broschyren Om krisen eller kriget kommer*. Myndigheten för samhällsskydd och beredskap. https://www.msb.se/sv/rad-till-privatpersoner/broschyren-om-krisen-eller-kriget-kommer/.

Myndigheten för psykologiskt försvar. (2022, 1. januar). *Uppdraget*. Hentet 6. mars 2022 fra https://www.mpf.se/vart-uppdrag/.

NCSC. (u.å.). *Five Eyes Intelligence Oversight and Review Council (FIORC)*. The National Counterintelligence and Security Center. Hentet 19. september 2022 fra https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc.

Nicholson, B. (2022). *EU looks to Australia for help on fighting foreign interference*. Australian Strategic Policy Institute (ASPI). Hentet 29. september 2022 fra https://www.aspistrategist.org.au/eu-looks-to-australia-for-help-on-fighting-foreign-interference/?utm_medium=email&utm_campaign=Weekly%20The%20Strategist&utm_content=Weekly%20The%20Strategist+CID_0741b4204171327594c8a1b2c8f39f84&utm_source=CampaignMonitor&utm_term=EU%20looks%20to%20Australia%20for%20help%20on%20fighting%20foreign%20interference.

NIM. (2021). *EMD med dom i to saker om digital nettovervåkning*. Norges Institusjon for menneskerettigheter (NIM). Hentet 19. september 2022 fra https://www.nhri.no/2021/emd-med-dom-i-to-saker-om-digital-nettovervakning/.

NOU 2021: 6. *Myndighetenes håndtering av koronapandemien. Rapport fra Koronakommisjonen.* Statsministeren.

Nye, J. S. J. (2017). Deterrence and dissuasion in cyberspace. *International Security*, *41*(3), 44-71.

OECD. (2021a). *Government at a Glance 2021*. https://www.oecd-ilibrary.org/content/publication/1c258f55-en.

OECD. (2021b). *Trust in government*. Organisation for Economic Co-operation and Development. Hentet 20. september 2022 fra https://data.oecd.org/gga/trust-in-government.htm.

Oma, I. M. (2021). *Avskrekking og beroligelse – den "doble strategi" som kom inn fra kulden* (IFS Insights 7/2021). Institutt for forsvarsstudier.

Ortiz-Ospina, E. & Roser, M. (2016). *Trust*. Our World in Data. Hentet 20. juni 2022 fra https://ourworldindata.org/trust.

Page, J., Lee, C. E. & Lubold, G. (2015). China's President Pledges No Militarization in Disputed Islands. *The Wall Street Journal*. https://www.wsj.com/articles/china-completes-runway-on-artificial-island-in-south-china-sea-1443184818.

Pamment, J. (2021). *RESIST 2 Counter Disinformation Toolkit*. UK Government Communication Service. https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

Pezard, S. & Rhoades, A. L. (2020). *What Provokes Putin's Russia? Deterring Without Unintended Escalation*. RAND Corporation. https://doi.org/10.7249/PE338.

Prop. 14 S (2020-2021). *Vilje til beredskap – evne til forsvar. Langtidsplan for forsvarssektoren* Forsvarsdepartementet.

Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. The Finnish Institute of International Affairs. https://www.fiia.fi/en/publication/russias-hybrid-war-in-ukraine.

Ramsay, G. & Robertshaw, S. (2019). *Weaponising News RT, Sputnik and targeted disinformation*. Centre for the Study of Media, Communication & Power. https://www.kcl.ac.uk/policy-institute/assets/weaponising-news.pdf.

Rauta, V. & Monaghan, S. (2021). Global Britain in the grey zone: Between stagecraft and statecraft. *Security Policy*, *42*, 475-497.

Regjeringen (Estland). (2017). *The National Security Concept of Estonia*. https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017_0.pdf.

Regjeringen (Estland). (2018, 15. februar 2018). *The government approved a comprehensive approach towards developing civil protection*. Hentet 15. september 2022 fra https://www.valitsus.ee/en/news/government-approved-comprehensive-approach-towards-developing-civil-protection.

Regjeringen (Estland). (2020). *About Government Office*. https://riigikantselei.ee/en/organisation-news-and-contacts/government-office/about-government-office.

Regjeringen (Estland). (u.å.). *Estonian National Defence 2022*. U. E. Forsvarsdepartementet (Estland). https://www.kaitseministeerium.ee/riigikaitse2022/index-en.html.

Regjeringen (Finland). (2016). *Government Report on Finnish Foreign and Security Policy*. P. M. s. O. Publications. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75139/VNKJ092016Government_report_on_kansineen_netti_enkku.pdf?sequence=1&isAllowed=y.

Regjeringen (Finland). (2021). *National security has improved along with legislation on intelligence*. Forsvarsdepartementet, Justisdepartementet, Innenriksdepartementet Hentet 19. september 2022 fra https://valtioneuvosto.fi/en/-//1410869/national-security-has-improved-along-with-legislation-on-intelligence.

Regjeringen (Sverige). (2020). *Summary of Government bill 'Totalförsvaret 2021–2025' (Total defence 2021–2025)*. Forsvarsdepartementet. Regjeringskansliet. https://www.government.se/4af8fa/globalassets/government/dokument/forsvarsdepartementet/ip-2021-2025/summary-of-government-bill-total-defence-2021-2025-final.pdf.

Rid, T. & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37.

Roepke, W.-D. & Thankey, H. (2019). *Resilience: the first line of defence*. NATO. Hentet 19. september 2022 fra https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Roser, M., Ritchie, H. & Ortiz-Ospina, E. (2013, May 2019). *World Population Growth*. Our World in Data. Hentet 20. juni 2022 fra https://ourworldindata.org/world-population-growth

Roth, A. (2018, 03.10.2018). Vladimir Putin calls Sergei Skripal a scumbag and a traitor. *The Guardian*. https://www.theguardian.com/uk-news/2018/oct/03/vladimir-putin-calls-sergei-skripal-a-scumbag-and-traitor.

Seebeck, L., Williams, E. & Wallis, J. (2022). *Countering the Hydra: A proposal for an Indo-Pacific hybrid threat centre*. Australian Strategic Policy Institute (ASPI). https://www.aspi.org.au/report/countering-hydra.

Sellevåg, S. R., Bergh, A., Bruvoll, J. A., Høibråten, S., Jacobsen, H. L., Strand, M. & Barland, B. (2021). *Samfunnsutvikling mot 2030 – utfordringer for politiet, PST og påtalemyndigheten* (FFI-rapport 21/01132). Forsvarets forskningsinstitutt.

SIS. (u.å.). *British Intelligence Explained*. Secret Intelligence Service (SIS) MI6. Hentet 19. september 2022 fra https://www.sis.gov.uk/intelligence-explained.html#section-00.

Skjelland, E., Berg-Knutsen, E., Arnfinnsson, B., Diesen, S., Glærum, S., Guttelvik, M. S., Kvalvik, S., Mørkved, T., Olsen, K. H., Sellevåg, S. R., Sendstad, C., Strand, K. R. & Voldhaug, J. E. (2022). *Forsvarsanalysen 2022* (FFI-rapport 22/00659). Forsvarets forskningsinstitutt.

Skjævesland, O. I. (2020). *Med økt spenning vokser militæret på Gotland*. Hentet 17. oktober 2022 fra https://forsvaretsforum.no/russland-sverige-utenriks/med-okt-spenning-vokser-militaeret-pa-gotland/163837.

Smith-Spark, L. & Polglase, K. (2018, 05.10.18). Netherlands officials say they caught Russian spies targeting chemical weapons body. *CNN*. https://edition.cnn.com/2018/10/04/europe/netherlands-russia-gru-intl/index.html.

Snyder, G. H. (1961). *Deterrence and Defense: Toward a Theory of National Security*. Princeton University Press.

Statsministerens kontor (Storbritannia). (2021). *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*. Cabinet Office. HM Government United Kingdom. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/975077/Global_Britain_in_a_Competitive_Age-_the_Integrated_Review_of_Security__Defence__Development_and_Foreign_Policy.pdf.

Stewart, J. (2022). The Grey Orchestra. *The RUSI Journal*, 1-12. https://doi.org/10.1080/03071847.2022.2075117.

Stoker, D. & Whiteside, C. (2020). Blurred Lines: Gray-Zone Conflict and Hybrid War - Two Failures of American Strategic thinking. *Naval War College Review, Vol. 73 [2020], No. 1, Art. 4*, *73*(4), 1-37, Artikkel 1 Winter 2020. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review.

Szymański, P. (2020). *New Ideas for Total Defence. Comprehensive Security in Finland and Estonia* (OSW Report 3/2020). OSW Centre for Eastern Studies. https://www.osw.waw.pl/sites/default/files/OSW-Report_New-ideas-for-total-defence_net_0.pdf.

Sørensen, H. & Nyemann, D. B. (2019). *Deterrence by Punishment as a way of Countering Hybrid Threats - Why we need to go 'beyond resilience' in the gray zone*. Hentet 15. mars 2022 fra https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783151/20190304-MCDC_CHW_Information_note_-_Deterrence_by_Punishment.pdf.

Takahashi, S. (2018). Development of gray-zone deterrence: concept building and lessons from Japan's experience. *The Pacific Review*, *31*(6), 787-810. https://doi.org/10.1080/09512748.2018.1513551.

The Economist Intelligence Unit. (2020). *Democracy Index 2020. In sickness and in health?*

The Security Committee. (2017). *The Security Strategy for Society* (Government Resolution / 2.11.2017).

Thies, C. G. (2002). A Pragmatic Guide to Qualitative Historical Analysis in the Study of International Relations. *International Studies Perspectives*, *3*(4), 351-372. http://www.jstor.org/stable/44218229.

Transparency International. (2021). *Corruption Perceptions Index*. Hentet 5. mars 2022 fra https://www.transparency.org/en/cpi/2021/.

UNEP & EU. (2022). *limate Change and Security Partnership Project - Final Report: March 2017 - February 2022*. https://wedocs.unep.org/20.500.11822/40549.

Utenriksdepartementet (Nederland). (2018). *Working Worldwide for the Security of the Netherlands: An Integrated International Security Strategy 2018-2022*. Utenriksdepartementet. Regjeringen (Nederland). https://www.almendron.com/tribuna/wp-content/uploads/2021/01/nl-international-integrated-security-strategy-2018-2022.pdf.

Veebel, V. & Ploom, I. (2018). Estonia's comprehensive approach to national defence: origins and dilemmas. *Journal on Baltic Security*, *4*, 10-22.

Veebel, V., Ploom, I. & Sazonov, V. (2022). Russian information warfare in Estonia, and Estonian countermeasures. *Lithuanian Annual Strategic Review*, *19*(1), 69-98. https://doi.org/10.47459/lasr.2021.19.4.

von Sydow, B. (2018, 4. april 2018). Resilience: Planning for Sweden's "Total Defence". *NATO REVIEW*. https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html.

Webster, J. & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii-xxiii. http://www.jstor.org/stable/4132319.

Wigell, M. (2019). Hybrid interference as a wedge strategy: a theory of external interference in liberal democracy. *International Affairs*, *95*(2), 255-275. https://doi.org/10.1093/ia/iiz018.

Wigell, M. (2021). Democratic Deterrence: How to Dissuade Hybrid Interference. *The Washington Quarterly*, *44*(1), 49-67. https://doi.org/10.1080/0163660X.2021.1893027.

Wigell, M., Hägglund, M., Fjäder, C., Hakala, E., Ketola, J. & Mikkola, H. (2022). *Nordic resilience. Strengthening cooperation on security of supply and crisis preparedness* (FIIA Report 70). Finnish Institute of International Affairs.

Wigell, M., Mikkola, H. & Juntunen, T. (2021). *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament: Directorate General for External Policies of the Union. https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653632.

Wijnja, K. (2022). Countering hybrid threats: does strategic culture matter? *Defence Studies*, *22*(1), 16-34. https://www.tandfonline.com/doi/pdf/10.1080/14702436.2021.1945452.

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections*, *15*(2), 73-87. http://www.jstor.org/stable/26326441.

Wither, J. K. (2020). Back to the future? Nordic total defence concepts. *Defence Studies*, *20*(1), 61-81. https://doi.org/10.1080/14702436.2020.1718498.

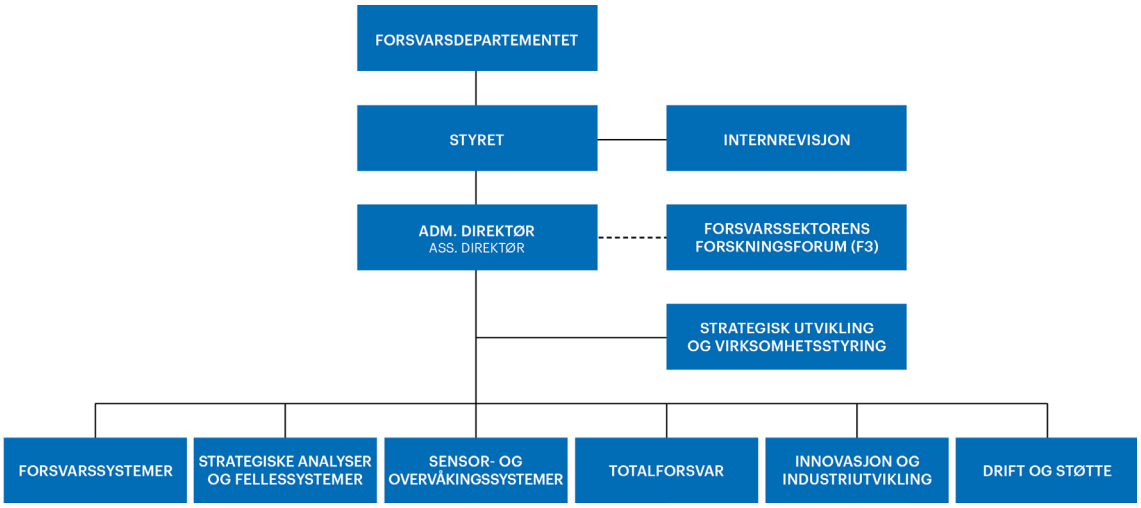
Zalnieriute, M. (2022). Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law*, *116*(3), 585-592. https://doi.org/10.1017/ajil.2022.35.

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